SOPHOS

SafeGuard® Enterprise 5.50
Administrator-Hilfe

Stand: November 2010

Inhalt

1 Das SafeGuard Management Center ... 3

2 Arbeitsschritte im Management Center ... 6

3 Aufbau der Organisationsstruktur ... 9

4 Mit mehreren Datenbankonfigurationen arbeiten ... 20

5 Unternehmenszertifikate und Zertifikat des Haupt-Sicherheitsbeauftragten exportieren ... 25

6 Lizenzen ... 29

7 SafeGuard Enterprise Sicherheitsbeauftragte ... 38

8 Datenverschlüsselung ... 63

9 SafeGuard Enterprise Schlüsselmanagement ... 67

10 Mit Richtlinien arbeiten ... 78

11 Mit Konfigurationspaketen arbeiten ... 95

12 Administrative Zugangsoptionen für Endpoint-Computer ... 96

13 Service Account Listen für die Windows-Anmeldung ... 97

14 POA Access Accounts für die POA-Anmeldung an Standalone-Computern ... 103

15 Sicherheitsrichtlinien ... 110

16 SafeGuard Configuration Protection ... 157

17 Benutzer-Computer Zuordnung ... 193

18 Token und Smartcards ... 198

19 SafeGuard Data Exchange 217

20 Die Power-on Authentication (POA) 226

21 Recovery-Optionen 238

22 Recovery über Local Self Help 240

23 Recovery über Challenge/Response 246

24 Systemwiederherstellung 272

25 Bestand- und Statusinformationen 278

26 Berichte 286

27 SafeGuard Enterprise und BitLocker-Laufwerkverschlüsselung 302

28 SafeGuard Enterprise und BitLocker To Go 308

29 Für Berichte auswählbare Ereignisse 310

30 Bedeutung der SGMERR-Codes in der Windows-Ereignisanzeige 319

31 Technischer Support 334

32 Copyright 335

1 Das SafeGuard Management Center

Das SafeGuard Management Center ist das zentrale Instrument zur Durchführung aller administrativen Tätigkeiten. Es greift auf eine Datenbank zu, in der alle relevanten Informationen gespeichert werden.

Mit datenbank-spezifischen Konfigurationen (Multi Tenancy) ermöglicht das SafeGuard Management Center den Einsatz von SafeGuard Enterprise mit mehreren Datenbanken und Domänen. Sie können verschiedene SafeGuard Enterprise Datenbanken verwalten und unterschiedliche Konfigurationen verwenden. Diese Konfigurationen können auch zur Vereinfachung der Konfiguration in Dateien exportiert und aus Dateien importiert werden.

Das SafeGuard Management Center muss nicht notwendigerweise nur auf einem Computer installiert sein. Es kann auf jedem Rechner im Netzwerk installiert sein, von wo aus auf die Datenbank zugegriffen werden kann.

Der Zugriff auf das SafeGuard Management Center ist nur privilegierten Benutzern - den Sicherheitsbeauftragten - erlaubt. Es können mehrere Sicherheitsbeauftragte gleichzeitig mit den Daten arbeiten.

1.1 Anmeldung an das SafeGuard Management Center

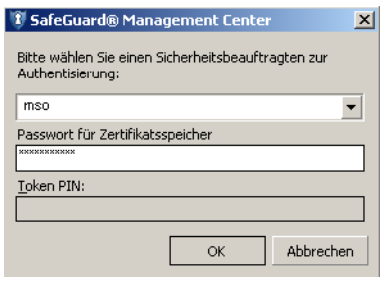
Bei der Installation und Konfiguration von SafeGuard Enterprise werden alle notwendigen Konfigurationseinstellungen ausgeführt. Außerdem wird ein Konto für den Haupt-Sicherheitsbeauftragten erstellt. Dieses Konto wird bei der ersten Anmeldung an das SafeGuard Management Center benötigt. Um das Management Center zu starten, benötigt der Benutzer das Kennwort für den Zertifikatsspeicher sowie den privaten Schlüssel des Zertifikats.

Weitere Informationen hierzu finden Sie im Installationshandbuch.

Die Anmeldung richtet sich danach, ob Sie das SafeGuard Management Center im Single Tenancy Modus oder im Multi Tenancy Modus einsetzen.

1.1.1 Anmeldung im Single Tenancy Modus

1. Starten Sie das SafeGuard Management Center über das **Start**-Menü. Ein Anmeldedialog wird angezeigt.



2. Melden Sie sich als Haupt-Sicherheitsbeauftragter an und geben Sie das Zertifikatsspeicherkennwort ein, das während der Konfiguration festgelegt wurde. Klicken Sie auf **OK**.

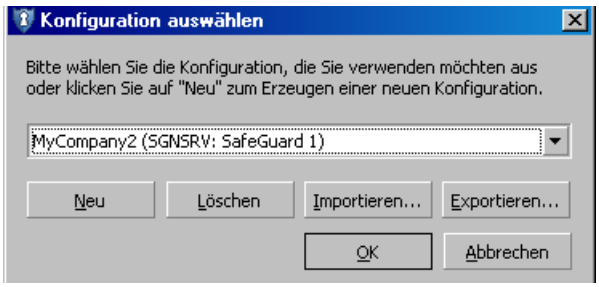
Hinweis: Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Nicht erfolgreiche Anmeldeversuche werden protokolliert.

Das SafeGuard Management Center wird geöffnet.

1.1.2 Anmeldung im Multi Tenancy Modus

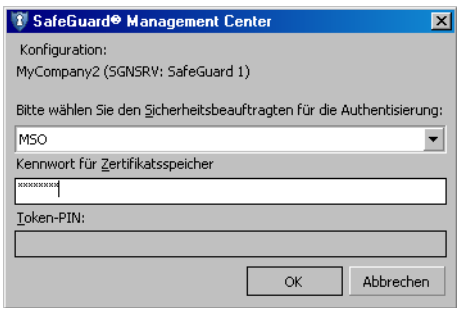
Wenn Sie mehrere Datenbanken konfiguriert haben (Multi Tenancy), erweitert sich der Anmeldevorgang, siehe *Mit mehreren Datenbankkonfigurationen arbeiten* auf Seite 20.

1. Starten Sie das SafeGuard Management Center über den Produktordner des **Start**-Menüs. Der Dialog **Konfiguration auswählen** wird angezeigt.



2. Wählen Sie die Datenbankkonfiguration, die Sie verwenden möchten, aus der Dropdownliste und klicken Sie auf **OK**. Die ausgewählte Datenbankkonfiguration wird mit dem Management Center verbunden und wird aktiv.

3. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Bestätigen Sie Ihre Angaben mit **OK**.



Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden.

Hinweis: Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Nicht erfolgreiche Anmeldeversuche werden protokolliert.

2 Arbeitsschritte im Management Center

Für den produktiven Einsatz von SafeGuard Enterprise sind folgende Schritte notwendig, damit die unternehmensweiten Sicherheitsrichtlinien auf dem Endpoint-Computer durchgesetzt werden können:

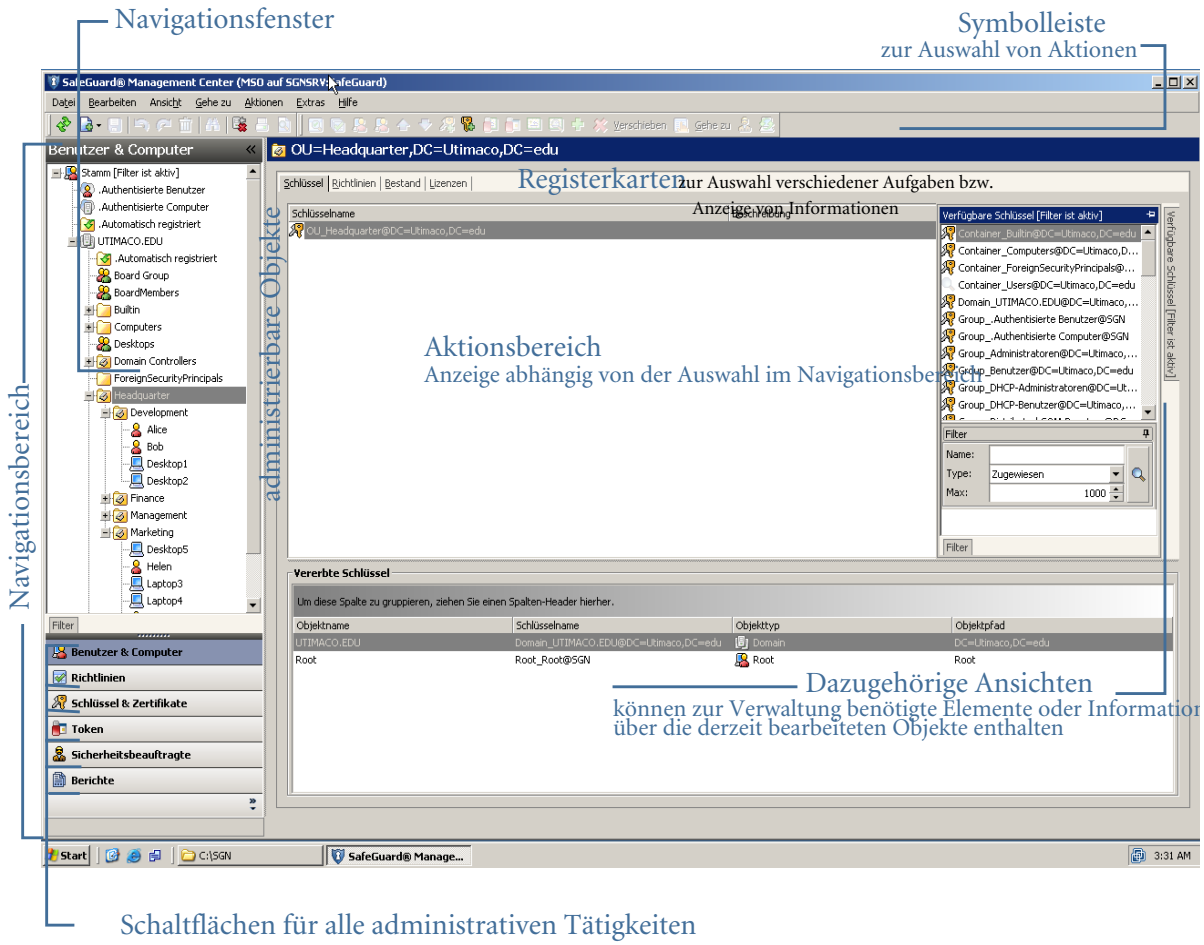
- Organisationsstruktur aufbauen oder importieren.
- Zusätzliche Sicherheitsbeauftragte anlegen.
- Erste (grundlegende) Richtlinien festlegen.
- In die Datenbank speichern
- Konfigurationen exportieren und importieren.

Alltagseinsatz

Nach der ersten Anmeldung lassen sich die Einstellungen beliebig erweitern. Die verschiedenen Sicherheitsbeauftragten können entsprechend den ihnen zugewiesenen Rollen Tätigkeiten ausführen.

Nach dem Speichern der neuen Einstellungen in der Datenbank können diese an die Endpoint-Computer übertragen werden, wo sie dann wirksam werden.

2.1 Der Arbeitsbereich des Management Centers



Navigationsbereich:

Im Navigationsbereich befinden sich Schaltflächen für alle administrativen Tätigkeiten:

- Benutzer & Computer

  Zum Importieren von Gruppen und Benutzern aus einem Active Directory, aus der Domäne oder von einem einzelnen Computer.

- Richtlinien

  Zum Erzeugen der Richtlinien.

- Schlüssel & Zertifikate

  Zum Verwalten der Schlüssel und Zertifikate.

- Token

  Zur Verwaltung von Token und Smartcards.

- Sicherheitsbeauftragte

  Zum Anlegen neuer Sicherheitsbeauftragter und Definieren von Aktionen, für deren Ausführung eine zusätzliche Autorisierung notwendig ist.

- Berichte

  Ermöglicht die Protokollierung aller sicherheitsrelevanten Ereignisse und deren Verwaltung.

Navigationsfenster

Abhängig davon, welche administrative Aufgabe über eine Schaltfläche gewählt wurde, werden im Navigationsfenster Objekte zur Bearbeitung angezeigt (Active Directory Objekte wie OUs, Benutzer und Computer; Richtlinien usw.) bzw. können dort erstellt werden.

Aktionsbereich

Hier werden die Einstellungen für das im Navigationsfenster ausgewählte Objekt vorgenommen. Im Aktionsbereich stehen verschiedene Registerkarten zur Verfügung mit deren Hilfe die Objekte bearbeitet und die Einstellungen vorgenommen werden können.

Informationen zu den ausgewählten Objekten werden ebenfalls im Aktionsbereich angezeigt.

Dazugehörige Ansichten (Associated Views):

In diesen Ansichten werden bei Bedarf zusätzliche Objekte und Informationen angezeigt. Diese geben einerseits nützliche Informationen bei der Verwaltung des Systems und unterstützen die einfache Bedienung. Zum Beispiel können Schlüssel über Drag & Drop Objekten zugewiesen werden.

Symbolleiste:

Hier befinden sich Symbole für die verschiedenen Aktionen im Management Center. Die Symbole werden eingeblendet, wenn sie für das ausgewählte Objekt zur Verfügung stehen.

Nach der Anmeldung wird das Management Center immer mit der Ansicht gestartet, in der es geschlossen wurde.

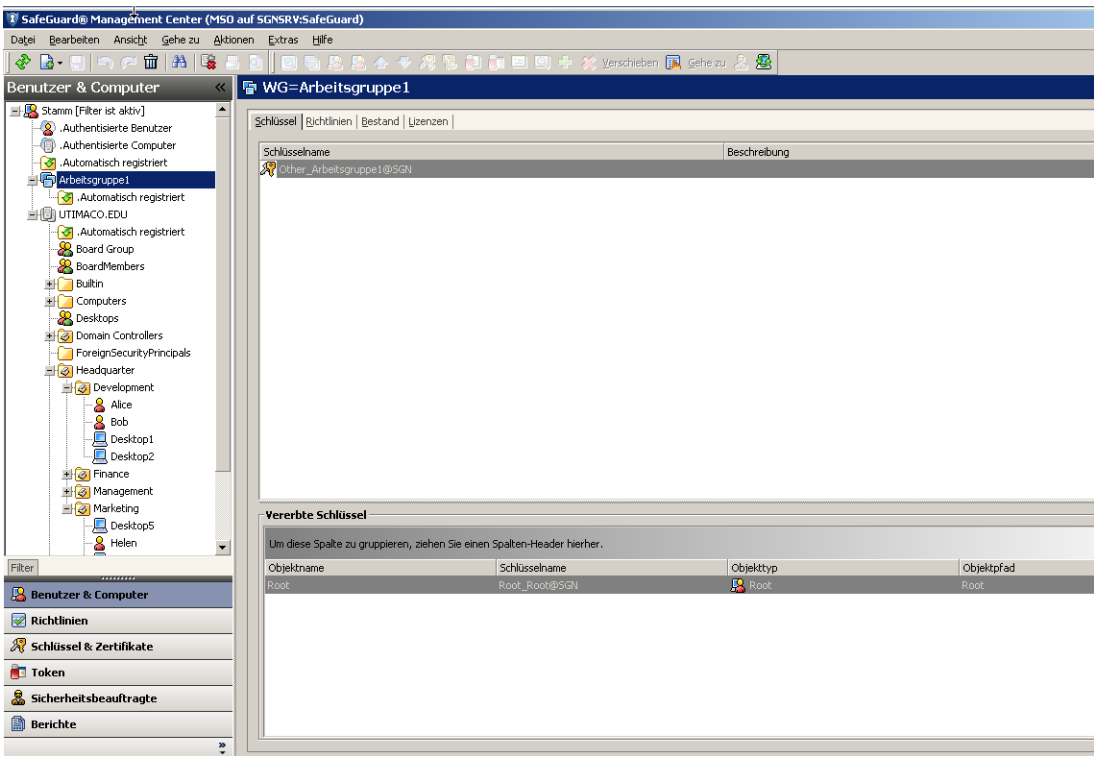
3 Aufbau der Organisationsstruktur

In SafeGuard Enterprise können Benutzer und Computer auch ohne den Import aus dem Active Directory erfasst werden. Wenn keine bestehende Organisationsstruktur vorhanden ist, kann sie in SafeGuard Enterprise schnell aufgebaut und eine Struktur zum Verwalten von Richtlinien aufgesetzt werden. Auch die Zuweisung von Richtlinien und/oder Verschlüsselungsregeln an lokale Benutzer ist dadurch möglich.

Der Sicherheitsbeauftragte mit den entsprechenden Rechten kann sogenannte Arbeitsgruppen oder noch nicht importierte Domänen einrichten, um die automatisch registrierten Benutzer und Computer zu verwalten.

Neue Benutzer/Computer, die sich an SafeGuard Enterprise anmelden, werden nach der ersten Synchronisierung mit der Datenbank im SafeGuard Management Center unter ihren entsprechenden Containern angezeigt. Danach kann der SO sie genau wie jedes importierte Objekt verwalten.

Das für diese Benutzer/Computer vorgesehene Verzeichnis .Automatisch registriert wird automatisch unterhalb des Stammverzeichnisses sowie unter jeder Domäne/Arbeitsgruppe erzeugt. Es kann nicht umbenannt oder verschoben werden. Objekte, die diesem Verzeichnis zugeordnet sind, können auch nicht manuell verschoben werden.



3.1 Sich als neuer Benutzer registrieren

Die Anmeldung eines neuen Benutzers erfolgt wie im Kapitel zur Power-on Authentication beschrieben (siehe *Die Power-on Authentication (POA)* auf Seite 200). Wenn sich ein neuer Benutzer zum ersten Mal an SafeGuard Enterprise anmeldet, wird bei der ersten Synchronisierung mit der Datenbank sein Status in der Datenbank geprüft und das neue Objekt entsprechend den Informationen in der Datenbank unter dem jeweiligen Container angezeigt. Wenn noch keine neue Arbeitsgruppe oder Domäne angelegt wurde, werden Benutzer im Verzeichnis .Automatisch registriert des Stammverzeichnisses angelegt. Wenn bereits eine Domäne angelegt wurde, der Benutzer/Computer aber noch nicht importiert wurde, werden sie im Verzeichnis .Automatisch registriert der Domäne hinzugefügt.

Hinweis: Lokale Benutzer können sich nicht mit einem leeren Kennwort an SafeGuard Enterprise anmelden. Wenn sich lokale Benutzer mit leerem Kennwort an SafeGuard Enterprise anmelden, bleiben sie Gäste und werden nicht in der Datenbank gespeichert.
Wenn für diese Benutzer zudem noch Windows Autologin aktiviert ist, wird die Anmeldung abgebrochen. Für die erfolgreiche Anmeldung an SafeGuard Enterprise muss in diesem Fall ein neues Kennwort vergeben werden und das Autologin für Windows in der Registry des Benutzer-Computers deaktiviert werden.

Anmelde-Informationen zu lokalem Objekt	Status in der Datenbank	Anzeige im Management Center
Lokaler Benutzer	Lokaler Benutzer nicht bekannt	unter Stammverzeichnis, .Automatisch registriert neu hinzugefügt unter seinem Computer
Lokaler Benutzer, Computer + Domäne	Domänenknoten bekannt Benutzer/Computer darin vorhanden	unter Domänenknoten bereits vorhanden
	Domänenknoten bekannt Benutzer/Computer darin nicht vorhanden	unter Domänenknoten, .Automatisch registriert neu hinzugefügt

Anmelde-Informationen zu lokalem Objekt	Status in der Datenbank	Anzeige im Management Center
Arbeitsgruppen-Computer + Arbeitsgruppe	Arbeitsgruppe bekannt Arbeitsgruppen-Computer darin physikalisch vorhanden	unter Arbeitsgruppe bereits vorhanden
	Arbeitsgruppe bekannt Name des Arbeitsgruppen-Computers darin unter .Automatisch registriert vorhanden	unter Arbeitsgruppe, .Automatisch registriert neu hinzugefügt **Achtung:** In diesem Fall müssen Sie prüfen, ob der Arbeitsgruppen-Computer zweimal in der Arbeitsgruppe vorhanden ist. Zur Unterscheidung identischer Computer gibt es unter **Eigenschaften** das Feld **Beschreibung**. Wir empfehlen jedoch, den Computer aus dem Verzeichnis .Automatisch registriert der Arbeitsgruppe manuell zu entfernen.
	Arbeitsgruppe bekannt Arbeitsgruppen-Computer darin nicht vorhanden	unter Arbeitsgruppe, .Automatisch registriert neu hinzugefügt
	Arbeitsgruppe nicht bekannt Arbeitsgruppen-Computer unter Stammverzeichnis, .Automatisch registriert bekannt	unter Stammverzeichnis, .Automatisch registriert bereits vorhanden
	Arbeitsgruppe nicht bekannt Arbeitsgruppen-Computer unter Stammverzeichnis, .Automatisch registriert unbekannt	unter Stammverzeichnis, .Automatisch registriert neu hinzugefügt
Domänen-Computer + Domäne	Domäne bekannt Domänen-Computer darin vorhanden	unter Domäne bereits vorhanden
	Domäne nicht bekannt	unter Stammverzeichnis, .Automatisch registriert neu hinzugefügt
	Domäne noch nicht synchronisiert	unter Domäne, .Automatisch registriert neu hinzugefügt

3.2 Anwendungsbeispiele für Auto-Registrierung

Im Folgenden finden Sie zwei Anwendungsbeispiele für das Verhalten von automatisch registrierten Objekten.

Beispiel 1: Benutzer/Computer außerhalb eines Active Directory verwalten

In einem Unternehmen müssen nicht zwangsläufig alle Benutzer/Computer Teil eines Active Directory (AD) sein, z. B. lokale Benutzer. Ein Unternehmen hat möglicherweise nur einen oder wenige Computer, so dass sich der Aufbau eines ADs nicht lohnt.

Dieses Unternehmen möchte SafeGuard Enterprise einsetzen, um dann seine Benutzer-/Computerobjekte mit Richtlinien zu versehen. Deshalb wird die Organisationsstruktur des Unternehmens im SafeGuard Management Center folgendermaßen manuell aufgebaut:

Benutzer & Computer Baum:

Stammverzeichnis

|_.Authentisierte Computer

|_.Authentisierte Benutzer

|_.Automatisch registriert

|_**BeispielArbeitsgruppe** (Eintrag manuell erzeugt)

|_.Automatisch registriert

|_**BeispielComputer001** (Eintrag erzeugt bei Anmeldung)

|_**BeispielComputer002** (Eintrag erzeugt bei Anmeldung)

|_...

Die Benutzer-/Computerobjekte bleiben im Verzeichnis .Automatisch registriert. Aber sie können im SafeGuard Management Center normal verwaltet werden (z. B. Richtlinien hinzufügen oder löschen).

Beispiel 2: SafeGuard Enterprise Datenbank und Active Directory nicht synchronisiert

Ein Benutzer oder Computer (SafeGuard Enterprise Client) ist bereits Teil eines Active Directory (AD) in einem Unternehmen. Jedoch sind die SafeGuard Enterprise Datenbank und das AD nicht synchronisiert: Benutzer und Computer werden im SafeGuard Management Center noch nicht angezeigt.

Der Benutzer meldet sich am Computer (SafeGuard Enterprise Client) mit folgenden Anmeldeinformationen an:

BeispielBenutzer

BeispielKennwort

BeispielDomäne

Diese Informationen werden an den SafeGuard Enterprise Server geschickt. Im SafeGuard Management Center werden dann folgende Einträge erzeugt:

Benutzer & Computer Baum:

Stammverzeichnis

|_.Authentisierte Computer

|_.Authentisierte Benutzer

|_.Automatisch registriert

|_**BeispielDomäne** (Eintrag erzeugt wenn mit AD synchronisiert)

|_.Automatisch registriert

|_**BeispielComputer** (Eintrag erzeugt bei Anmeldung)

|_**BeispielBenutzer** (Eintrag erzeugt bei Anmeldung)

Mit der nächsten Synchronisierung zwischen dem AD und der SafeGuard Enterprise Datenbank werden **BeispielComputer** und **BeispielBenutzer** automatisch in ihre korrekten Organisationseinheiten (OU) verschoben.

Der Sicherheitsbeauftragte kann dem Verzeichnis .Automatisch registriert zwar Richtlinien zuweisen, aber diese Richtlinien gelten nur für den **BeispielComputer** und den **BeispielBenutzer,** so lange diese Objekte sich im Verzeichnis .Automatisch registriert befinden.

Sobald die Objekte durch die Synchronisierung zwischen AD und der SafeGuard Enterprise Datenbank in ihre Organisationseinheiten (OU) verschoben werden, gelten hingegen für den **BeispielComputer** und den **BeispielBenutzer** die Richtlinien dieser OUs.

3.3 Schlüssel und Zertifikate für autoregistrierte Objekte

Für jedes autoregistrierte Objekt wird vom Server bei Bedarf ein Zertifikat erstellt.

Ein lokaler Benutzer erhält zwei Schlüssel:

- den Schlüssel des Containers .Automatisch registriert
- den privaten Schlüssel, der vom Server bei Bedarf erzeugt wird.

Lokale Benutzer erhalten keine weiteren Schlüssel der ihnen übergeordneten Container, auch keinen Root-Schlüssel.

Arbeitsgruppen erhalten gar keine Schlüssel.

3.4 Richtlinien für autoregistrierte Objekte

Für autoregistrierte Objekte können ohne Einschränkung Richtlinien erstellt werden.

Lokale Benutzer werden zur Gruppe „.authentisierte Benutzer“ hinzugefügt. Computer werden zur Gruppe „.authentisierte Computer“ hinzugefügt. Dementsprechend gelten für sie die Richtlinien, die für diese Gruppe aktiviert wurden.

3.5 Neue Arbeitsgruppe erstellen

Als SO können Sie unter dem Stammverzeichnis einen Container erzeugen, der eine Windows Arbeitsgruppe repräsentiert. Arbeitsgruppen erhalten keine Schlüssel. Sie können nicht umbenannt werden.

1. Klicken Sie im SafeGuard Management Center auf den Bereich **Benutzer & Computer**.
2. Rechts-klicken Sie im linken Navigationsfenster auf **Stamm [Filter ist aktiv]** und wählen Sie **Neu > Neue Arbeitsgruppe erzeugen (autom. Registrierung)**.
3. Machen Sie in **Allgemeine Informationen** folgende Angaben
   a) **Vollst. Name:** Namen für die Arbeitsgruppe
   b) Sie können optional eine **Beschreibung** der Arbeitsgruppe einfügen.
   c) Unter **Verbindungsstatus** wird der Typ des Objekts angezeigt, in diesem Fall `Arbeitsgruppe`.
   d) Klicken Sie auf **Richtlinienvererbung stoppen**, wenn Richtlinien nicht vererbt werden sollen.
   e) Bestätigen Sie die Angaben mit **OK**.

Die Arbeitsgruppe ist nun erzeugt. Unterhalb des Arbeitsgruppen-Containers wird automatisch das Standardverzeichnis .Automatisch registriert angelegt. Es kann weder umbenannt noch gelöscht werden.

3.6 Arbeitsgruppe löschen

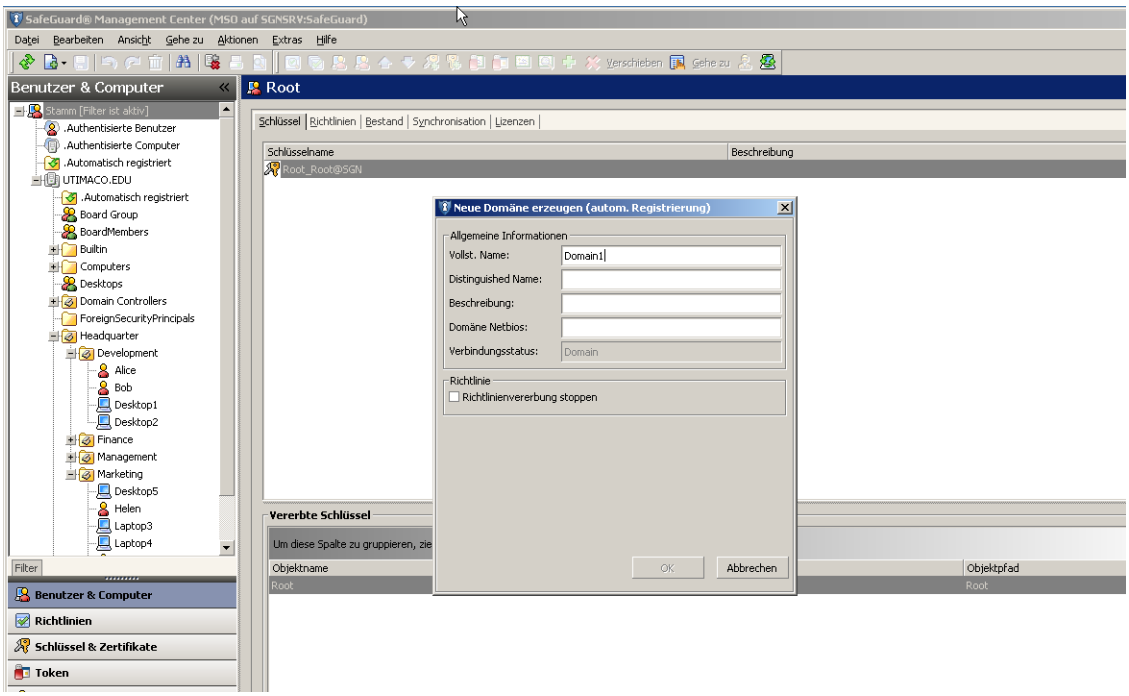
Als SO können Sie Arbeitsgruppen löschen. Falls die Arbeitsgruppe Mitglieder hatte, werden diese ebenfalls gelöscht. (Bei der nächsten Anmeldung werden sie wieder autoregistriert).

1. Klicken Sie im SafeGuard Management Center auf den Bereich **Benutzer & Computer**.
2. Rechts-klicken Sie im rechten Navigationsbereich die Arbeitsgruppe, die gelöscht werden soll und wählen Sie **Löschen**. Bestätigen Sie mit **Ja**.

Die Arbeitsgruppe ist nun gelöscht. Eventuelle Mitglieder werden ebenfalls gelöscht.

3.7 Neue Domäne erstellen

Als SO mit den nötigen Berechtigungen können Sie unter dem Stammverzeichnis eine neue Domäne anlegen. Sie sollten nur neue Domänen anlegen, wenn Sie keine Domänen aus dem Active Directory (AD) importieren wollen oder können, z. B. weil kein AD vorhanden ist.



1. Klicken Sie im SafeGuard Management Center auf den Bereich **Benutzer & Computer**.

1. Rechts-klicken Sie im linken Navigationsfenster auf **Stamm [Filter ist aktiv]** und wählen Sie im Kontextmenü **Neu > Neue Domäne erzeugen (autom. Registrierung)**.

2. In **Allgemeine Informationen** machen Sie folgende Angaben zum Domänen-Controller. Alle drei Namenseingaben müssen korrekt sein, sonst wird die Domäne nicht synchronisiert:

   a) **Vollst. Name**: z. B. *rechnername.domäne.com* oder die IP-Adresse des Domänen-Controllers

   b) **Distinguished Name**: DNS-Name, z. B. `DC=rechnername3,DC=domäne,DC=Land`

   c) Beschreibung der Domäne (optional)

   d) **Domäne Netbios**: Name des Domänen-Controllers

   e) Unter **Verbindungsstatus** wird der Typ des Objekts angezeigt, in diesem Fall `Domäne`.

   f) Klicken Sie auf **Richtlinienvererbung stoppen**, wenn Richtlinien nicht vererbt werden sollen.

   g) Bestätigen Sie die Angaben mit **OK**.

Die Domäne ist nun neu angelegt. Ein Benutzer und/oder ein Computer wird bei der Autoregistrierung automatisch dieser Domäne zugeordnet. Unterhalb des Domänen-Containers wird das Standardverzeichnis .Automatisch registriert angelegt. Es kann weder umbenannt noch gelöscht werden.

3.8 Domäne umbenennen

Als Sicherheitsbeauftragter mit den nötigen Berechtigungen können Sie eine Domäne umbenennen und weitere Eigenschaften für sie festlegen.

1. Klicken Sie im SafeGuard Management Center auf den Bereich **Benutzer & Computer**.
2. Rechts-klicken Sie im linken Navigationsfenster auf die Domäne, die Sie umbenennen möchten und wählen Sie im Kontextmenü **Eigenschaften**.
3. Ändern Sie in **Allgemeine Informationen** unter **Vollst. Name** den Namen der Domäne und evtl. die Beschreibung.
4. In **Domäne NetBios** können Sie den Namen des Domänen-Controllers ändern.
5. Außerdem können Sie in der Registerkarte **Containereinstellungen** den Wake-on-LAN-Modus für den automatischen Neustart festlegen.
6. Bestätigen Sie mit **OK**.

Die Änderungen sind nun gespeichert.

3.9 Domäne löschen

Als SO mit den nötigen Berechtigungen können Sie Domänen löschen. Falls die Domäne Mitglieder hatte, werden diese ebenfalls gelöscht.

1. Klicken Sie im SafeGuard Management Center auf den Bereich **Benutzer & Computer**.
1. Rechts-klicken Sie im linken Navigationsfenster die Domäne, die gelöscht werden soll und wählen Sie **Löschen**. Bestätigen Sie mit **Ja**.

Die Domäne ist nun gelöscht. Eventuelle Mitglieder werden ebenfalls gelöscht.

3.10 Automatisch registrierte Computer löschen

Wenn ein automatisch registrierter Computer gelöscht wird, werden alle lokalen Benutzer dieses Computers ebenfalls gelöscht. Bei der nächsten Anmeldung dieses Computers wird er erneut automatisch registriert.

3.11 Filter für lokale Objekte

Benutzer & Computer

Unter **Benutzer & Computer** können Sie die Ansicht im linken Navigationsfenster nach lokalen Benutzern filtern oder einen bestimmten lokalen Benutzer suchen.

1. Klicken Sie im SafeGuard Management Center auf den Bereich **Benutzer & Computer**.
2. Klicken Sie links unten im Navigationsbereich auf **Filter**.
3. Aktivieren Sie **Lokaler Benutzer**. Wenn Sie einen bestimmten Benutzer suchen, geben Sie noch dessen Namen ein.
4. Klicken Sie auf das Lupen-Symbol.

Die Ansicht auf **Benutzer & Computer** wird entsprechend den Kriterien gefiltert.

Protokollierung

Die erfolgreiche bzw. nicht erfolgreiche Registrierung eines Benutzers, Computers oder einer Arbeitsgruppe wird protokolliert. Sie können sich diese Informationen im SafeGuard Management Center unter **Berichte** in der Ereignisanzeige auflisten lassen.

3.12 Import der Organisationsstruktur über Active Directory

Eine bereits bestehende Organisationsstruktur, z. B. ein Active Directory, kann in SafeGuard Enterprise importiert und dann verwaltet werden.

1. Wählen Sie im SafeGuard Management Center **Extras > Optionen.**
2. Wählen Sie die Registerkarte **Verzeichnis** und klicken Sie auf **Hinzufügen**.
3. Gehen Sie in **LDAP Authentisierung** folgendermaßen vor:
   a) Bei **Servername oder IP** geben Sie den NetBIOS-Name des Domänencontrollers oder dessen IP ein.
   b) Bei **Benutzername und Kennwort** geben Sie Ihre Windows-Anmeldeinformationen zur (Test-)Umgebung ein.
   c) Bestätigen Sie mit **OK**.

Hinweis: Bei Windows Einzelplatzcomputern muss auf dem PC ein Verzeichnis freigegeben sein, damit eine Verbindung via LDAP möglich wird.

4. Klicken Sie auf **Benutzer & Computer**.

5. Klicken Sie im linken Navigationsfenster auf das Stammverzeichnis **Stamm [Filter ist aktiv]**.
6. Wählen Sie im rechten Aktionsbereich die Registerkarte **Synchronisation**.
7. Wählen Sie aus dem **Verzeichnis DSN** das gewünschte Verzeichnis aus. Klicken Sie auf das Lupensymbol rechts oben. Es erscheint eine Abbildung der Active Directory-Struktur der Organisationseinheiten (OU) in Ihrem Unternehmen.
8. Es muss nicht der gesamte Inhalt des Active Directory importiert werden. Markieren Sie die Organisationseinheiten (OU), die synchronisiert werden sollen.
9. Klicken Sie unten im Aktionsbereich auf **Synchronisieren**.

Hinweis: Bei der Synchronisierung von Benutzern und deren Gruppen-Zugehörigkeiten wird die Zugehörigkeit zu einer "primary group" nicht synchronisiert, da diese Zugehörigkeit nicht in der Gruppe aufscheint.

Die Domänen werden synchronisiert und Details der Synchronisierung werden angezeigt. Die Fortschrittsanzeige links unten in der Statusleiste zeigt ein Synchronisierungsprotokoll an. Wenn Sie auf diese Anzeige klicken, können Sie das Synchronisierungsprotokoll kopieren und zum Beispiel in eine E-Mail oder eine Datei kopieren, um Ihre Benutzer über die Ergebnisse der Synchronisierung zu informieren.

3.13 Eine neue Domäne aus einem Active Directory importieren

Wenn Sie nur eine neue Domäne aus dem Active Directory importieren möchten, gehen Sie wie folgt vor:

1. Klicken Sie im linken Navigationsfenster auf das Stammverzeichnis **Stamm [Filter ist aktiv]**.
2. Wählen Sie **Datei > Neu > Neue Domäne aus AD importieren**.
3. Wählen Sie im rechten Aktionsbereich die Registerkarte **Synchronisation**.
4. Wählen Sie das gewünschte Verzeichnis aus der **Verzeichnis DSN** Liste. Klicken Sie auf das Lupensymbol rechts oben. Es erscheint eine Abbildung der Active Directory-Struktur der Organisationseinheiten (OU) in Ihrem Unternehmen.
5. Wählen Sie die Domäne, die synchronisiert werden soll und klicken Sie auf **Synchronisieren**.

4 Mit mehreren Datenbankkonfigurationen arbeiten

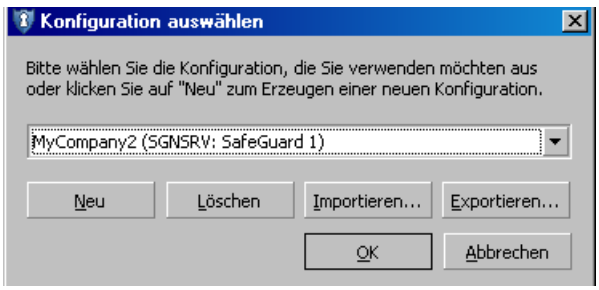
Das SafeGuard Management Center ermöglicht die Benutzung mehrerer Datenbankkonfigurationen (Multi Tenants). Wenn Sie diese Funktion nutzen möchten, müssen Sie sie während der Installation aktivieren. Detaillierte Informationen hierzu finden Sie im SafeGuard Enterprise Installationshandbuch.

Mit Multi Tenancy können Sie verschiedene SafeGuard Enterprise Datenbankkonfigurationen konfigurieren und sie für eine Instanz des SafeGuard Management Centers verwalten. Dies erweist sich vor allem dann als nützlich, wenn Sie verschiedene Konfigurationen für verschiedene Domänen, OUs oder Unternehmensstandorte einsetzen möchten.

Voraussetzung: Die Funktion Multi Tenancy muss über eine Installation vom Typ Angepasst installiert worden sein. Die initiale Konfiguration muss durchgeführt worden sein. Detaillierte Informationen hierzu finden Sie im SafeGuard Enterprise Installationshandbuch.

Zur Vereinfachung der Konfiguration haben Sie folgende Möglichkeiten:

- Mehrere Datenbank-Konfigurationen erstellen.
- Zuvor erstellte Datenbankkonfigurationen auswählen.
- Zuvor erstellte Datenbankkonfiguration aus einer Datei importieren.
- Datenbankkonfiguration zur späteren Wiederverwendung exportieren.



4.1 Weitere Datenbankkonfigurationen erstellen

So erstellen Sie eine weitere SafeGuard Enterprise Datenbankkonfiguration nach der initialen Konfiguration:

1. Starten Sie das SafeGuard Management Center. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Klicken Sie auf **Neu**. Der SafeGuard Management Center Konfigurationsassistent wird automatisch gestartet.

3. Der Assistent führt Sie durch die notwendigen Schritte für das Anlegen einer neuen Datenbankkonfiguration. Nehmen Sie die erforderlichen Einstellungen vor. Die neue Datenbankkonfiguration wird generiert.

4. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Bestätigen Sie Ihre Angaben mit **OK**.

Das SafeGuard Management Center wird geöffnet und mit der neuen Datenbankkonfiguration verbunden. Wenn Sie das SafeGuard Management Center das nächste Mal starten, können Sie die neue Datenbank-Konfiguration aus der Liste auswählen.

4.2 Mit bereits vorhandener Datenbankkonfiguration verbinden

So benutzen Sie eine bereits vorhandene SafeGuard Enterprise Datenbankkonfiguration:

1. Starten Sie das SafeGuard Management Center. Der Dialog **Konfiguration auswählen** wird angezeigt.

2. Wählen Sie die Datenbankkonfiguration, die Sie verwenden möchten, aus der Dropdownliste und klicken Sie auf **OK**. Die ausgewählte Datenbankkonfiguration wird mit dem SafeGuard Management Center verbunden und wird aktiv.

3. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Bestätigen Sie Ihre Angaben mit **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden.

4.3 Konfiguration in eine Datei exportieren

Um eine Konfiguration zu speichern, damit sie später wiederverwendet werden kann, können Sie sie in eine Datei exportieren. Gehen Sie hierzu wie folgt vor:

1. Starten Sie das SafeGuard Management Center. Der Dialog **Konfiguration auswählen** wird angezeigt.

2. Klicken Sie auf **Exportieren...**

3. Zum Schutz der Konfigurationsdatei werden Sie dazu aufgefordert, ein Kennwort einzugeben und zu bestätigen, das die Konfigurationsdatei verschlüsselt. Klicken Sie auf **OK**.

4. Geben Sie einen Dateinamen und einen Speicherort für die exportierte Konfigurationsdatei *.SGNConfig an.
5. Sollte diese Konfiguration bereits vorhanden sein, so werden Sie gefragt, ob Sie die vorhandene Konfiguration überschreiben möchten.

Die Datenbankkonfiguration wird am angegebenen Speicherort gespeichert.

4.4 Konfiguration importieren

Um eine Datenbankkonfiguration zu verwenden oder zu ändern, können Sie eine zuvor erstellte Konfiguration in das SafeGuard Management Center importieren. Hier gibt es zwei Möglichkeiten:

- über das SafeGuard Management Center (für Multi Tenancy)
- durch Doppelklicken auf die Konfigurationsdatei (für Single und Multi Tenancy)

4.5 Konfiguration über das SafeGuard Management Center importieren

1. Starten Sie das SafeGuard Management Center. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Klicken Sie auf **Import...**, wählen Sie die gewünschte Konfigurationsdatei aus und klicken Sie auf **Öffnen**.
3. Geben Sie das Kennwort ein, das während des Exports für die Konfigurationsdatei erstellt wurde, und klicken Sie auf **OK**.
4. Die ausgewählte Konfiguration wird angezeigt. Um zu bestätigen, dass diese Konfiguration aktiviert werden soll, klicken Sie auf **OK**.
5. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Bestätigen Sie Ihre Angaben mit **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden.

4.6 Konfiguration durch Doppelklicken auf die Konfigurationsdatei importieren (Single und Multi Tenancy)

Hinweis: Dieser Vorgang ist sowohl im Single Tenancy als auch im Multi Tenancy Modus möglich.

Es besteht auch die Möglichkeit, eine Konfiguration zu exportieren und diese an mehrere Sicherheitsbeauftragte zu verteilen. Die Sicherheitsbeauftragten müssen lediglich auf die Konfigurationsdatei doppelklicken, um ein vollständig konfiguriertes SafeGuard Management Center zu öffnen.

Dies erweist sich vor allem dann als vorteilhaft, wenn Sie die SQL Authentisierung für die Datenbank verwenden und vermeiden möchten, dass das SQL-Kennwort jedem Administrator bekannt ist. Sie müssen das Kennwort dann nur einmal eingeben, eine Konfigurationsdatei erstellen und sie an die Computer der Sicherheitsbeauftragten verteilen.

Voraussetzung: Die initiale Konfiguration des SafeGuard Management Centers muss durchgeführt worden sein. Detaillierte Informationen hierzu finden Sie im SafeGuard Enterprise Installationshandbuch.

1. Starten Sie das SafeGuard Management Center über den Produktordner im **Start**-Menü.
2. Wählen Sie im **Extras**-Menü **Optionen** und wechseln Sie in die Registerkarte **Datenbank**.
3. Geben Sie die Anmeldeinformationen für die Verbindung zum SQL Datenbankserver ein oder bestätigen Sie diese.
4. Klicken Sie auf **Konfiguration exportieren**, um die Konfiguration in eine Datei zu exportieren.
5. Geben Sie ein Kennwort für die Konfigurationsdatei ein und bestätigen Sie es.
6. Geben Sie einen Dateinamen ein und wählen Sie einen Speicherort aus.
7. Verteilen Sie die Konfigurationsdatei an die Computer der Sicherheitsbeauftragten. Teilen Sie ihnen das Kennwort für diese Datei sowie das Zertifikatsspeicherkennwort mit, das Sie für Anmeldung an das SafeGuard Management Center benötigen.
8. Die Sicherheitsbeauftragten müssen nur auf die Konfigurationsdatei doppelklicken.
9. Sie werden aufgefordert, das Kennwort für die Konfigurationsdatei einzugeben.
10. Zur Anmeldung an das SafeGuard Management Center werden die Sicherheitsbeauftragten aufgefordert, ihr Zertifikatsspeicherkennwort einzugeben.

Das SafeGuard Management Center startet mit der importierten Konfiguration. Diese Konfiguration wird nun als neue Standardkonfiguration definiert.

4.7 Schneller Wechsel zwischen Datenbankkonfigurationen

Zur Vereinfachung von Verwaltungsaufgaben bei mehreren Datenbanken bietet das SafeGuard Management Center den schnellen Wechsel zwischen Datenbankkonfigurationen.

So wechseln Sie zu einer anderen Datenbankkonfiguration:

1. Wählen Sie **Datei** in der Menüleiste des Management Centers und klicken Sie auf **Konfiguration wechseln...**
2. Wählen Sie die Datenbank, zu der Sie wechseln möchten, aus der Dropdownliste aus und bestätigen Sie mit **OK**.

Das Management Center wird automatisch mit der ausgewählten Konfiguration neu gestartet.

Hinweis: Dieser Vorgang ist auch im Single Tenancy Modus möglich.

4.8 Datenbankintegrität prüfen

Bei der Anmeldung an die Datenbank wird die Datenbankintegrität automatisch geprüft. Sollte diese Überprüfung Fehler ergeben, wird der Dialog **Datenbankintegrität prüfen** angezeigt.

Sie können die Datenbankintegrität auch jederzeit nach der Anmeldung prüfen und hierzu den Dialog **Datenbankintegrität prüfen** aufrufen:

1. Wählen Sie **Extras > Datenbankintegrität** in der Menüleiste des SafeGuard Management Centers.
2. Um die Tabellen zu prüfen, klicken Sie auf **Alle prüfen** oder **Ausgewählte prüfen**. Danach werden fehlerhafte Tabellen im Dialog markiert.

Um die Fehler zu beheben, klicken Sie auf **Reparieren**.

5 Unternehmenszertifikate und Zertifikat des Haupt-Sicherheitsbeauftragten exportieren

In einer SafeGuard Enterprise Installation sind die beiden folgenden Elemente von entscheidender Bedeutung und erfordern daher die Erstellung von Backups an einem sicheren Speicherort:

- das in der SafeGuard-Datenbank gespeicherte Unternehmenszertifikat
- das Zertifikat des Haupt-Sicherheitsbeauftragten (MSO) im Zertifikatsspeicher des Computers, auf dem das SafeGuard Management Center installiert ist.

Beide Zertifikate lassen sich als .p12 Dateien zur Erstellung von Sicherungskopien exportieren. Installationen lassen sich dann durch Importieren des relevanten Unternehmenszertifikats sowie des Zertifikats des Haupt-Sicherheitsbeauftragten als P12-Dateien wiederherstellen. Die Zertifikate können beim Anlegen einer neuen Datenbank verwendet werden. Das Wiederherstellen einer Sicherungskopie der gesamten Datenbank ist somit nicht notwendig.

Hinweis: Wir empfehlen, diesen Vorgang direkt nach der Erstkonfiguration des SafeGuard Management Center auszuführen.

5.1 Zertifikat des Haupt-Sicherheitsbeauftragten exportieren

Um ein Backup des Zertifikats des derzeit am SafeGuard Management Center angemeldeten Haupt-Sicherheitsbeauftragten zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie **Extras > Optionen** in der SafeGuard Management Center Menüleiste.
2. Wechseln Sie in die Registerkarte **Zertifikate** und klicken Sie im Bereich **<Administrator> Zertifikat** auf **Exportieren** .
3. Sie werden dazu aufgefordert, ein Kennwort für die Sicherung der exportierten Datei einzugeben. Geben Sie ein Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
4. Geben Sie einen Dateinamen und eine Speicherort für die zu exportierende Datei ein und klicken Sie auf **OK**.

Das Zertifikat des derzeit angemeldeten Hauptsicherheitsbeauftragten wird als P12-Datei an den definierten Speicherort exportiert und kann für Recovery-Vorgänge benutzt werden.

5.2 Unternehmenszertifikate exportieren

Hinweis: Nur Haupt-Sicherheitsbeauftragte sind dazu berechtigt, Unternehmenszertifikate zur Erstellung eines Backups zu exportieren.

1. Wählen Sie **Extras > Optionen** in der SafeGuard Management Center Menüleiste.
2. Wechseln Sie in die Registerkarte **Zertifikate** und klicken Sie im Bereich **Unternehmenszertifikat** auf **Exportieren**.
3. Sie werden dazu aufgefordert, ein Kennwort für die Sicherung der exportierten Datei einzugeben. Geben Sie ein Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
4. Geben Sie einen Dateinamen und einen Speicherort für die zu exportierende Datei ein und klicken Sie auf **OK**.

Das Unternehmenszertifikat wird als P12-Datei an den definierten Speicherort exportiert und kann für Recovery-Vorgänge benutzt werden.

5.3 Korrupte SafeGuard Management Center Installation wiederherstellen

Eine korrupte SafeGuard Management Center Installation kann auf einfache Art und Weise wiederhergestellt werden, wenn die Datenbank noch intakt ist. In diesem Fall müssen Sie nur das SafeGuard Management Center neu installieren und die vorhandene Datenbank sowie das gesicherte Sicherheitsbeauftragten-Zertifikat verwenden.

Gehen Sie wie folgt vor:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie unter **Datenbankverbindung** den relevanten Datenbankserver und konfigurieren Sie, falls erforderlich, die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Aktivieren Sie unter **Datenbankeinstellungen** die Option**Folgende bestehende Datenbank verwenden** und wählen Sie die Datenbank aus der Liste aus.
4. Führen Sie unter **Daten des Sicherheitsbeauftragten** einen der folgenden Schritte aus:
   - Wenn die gesicherte Zertifikatdatei auf dem Computer gefunden wird, wird sie angezeigt. Geben Sie das Kennwort ein, das Sie zur Anmeldung an das SafeGuard Management Center benutzen.

- Wird die gesicherte Zertifikatdatei nicht auf dem Computer gefunden, klicken Sie auf **Importieren**. Suchen Sie nach der gesicherten Zertifikatdatei und bestätigen Sie Ihre Auswahl mit **Öffnen**. Geben Sie das Kennwort für die ausgewählte Zertifikatdatei ein.Bestätigen Sie das Kennwort mit **Ja**. Geben Sie ein Kennwort für die Anmeldung am SafeGuard Management Center ein und bestätigen Sie es.

5. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um die Konfiguration des SafeGuard Management Center abzuschließen.

Die SafeGuard Management Center Installation ist wiederhergestellt.

5.4 Korrupte Datenbankkonfiguration wiederherstellen

Sie können eine korrupte Datenbankkonfiguration wiederherstellen, indem Sie das SafeGuard Management Center neu installieren und basierend auf den gesicherten Zertifikatsdateien einen neue Instanz der Datenbank erstellen. Dadurch wird sichergestellt, dass alle vorhandenen, durch SafeGuard Enterprise geschützten Computer Richtlinien von der neuen Installation annehmen. Somit müssen Sie nicht die gesamte Datenbank neu einrichten und wiederherstellen.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein.
- Die Kennwörter für die beiden .p12 Dateien sowie für den Zertifikatsspeicher müssen Ihnen bekannt sein.

Gehen Sie wie folgt vor:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie unter **Datenbank-Verbindung** die Option **Neue Datenbank erstellen**. Konfigurieren Sie unter **Datenbankeinstellungen** die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Wählen Sie unter **Daten des Sicherheitsbeauftragten** den relevanten Haupt-Sicherheitsbeauftragten und klicken Sie auf **Importieren**.
4. Suchen Sie unter **Importieren des Zertifikats** die gesicherte Zertifikatsdatei. Geben Sie unter **Schlüsseldatei** das für diese Datei festgelegte Kennwort ein und bestätigen Sie es. Klicken Sie auf **OK**.
5. Das Zertifikat des Haupt-Sicherheitsbeauftragten wird importiert. Klicken Sie auf **Weiter**.

6. Aktivieren Sie unter **Unternehmenszertifikat** die Option **Über vorhandenes Unternehmenszertifikat wiederherstellen**. Klicken Sie auf **Importieren**, um die gesicherte Zertifikatsdatei auszuwählen, die das gültige Unternehmenszertifikat enthält. Sie werden dazu aufgefordert, das für den Zertifikatsspeicher festgelegte Kennwort einzugeben. Geben Sie das Kennwort ein und bestätigen Sie es mit **OK**. Bestätigen Sie die angezeigte Meldung mit **Ja**. Das Unternehmenszertifikat wird importiert.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Die Datenbankkonfiguration ist wiederhergestellt.

6 Lizenzen

Für die Nutzung des SafeGuard Enterprise Management Centers im produktiven Betrieb ist eine gültige Lizenz erforderlich. So ist eine gültige Lizenz in der SafeGuard Enterprise Datenbank zum Beispiel die Voraussetzung für die Übertragung von Richtlinien an die Benutzer-Computer. Darüber hinaus sind für die Token-Verwaltung die entsprechenden Token-Lizenzen notwendig.

Von Ihrem Vertriebspartner erhalten Sie Ihre Kunden-Lizenzdatei zum Import in die SafeGuard Enterprise Datenbank nach der Installation. Die Lizenzdatei enthält u.a. Informationen zur Anzahl an erworbenen Lizenzen pro Modul/Name des Lizenzinhabers sowie ein festgelegtes Toleranzlimit für die Lizenzüberschreitung. Bei Überschreiten der verfügbaren Lizenzen bzw. des Toleranzlimits werden beim Starten des SafeGuard Management Centers entsprechende Warnungs- bzw. Fehlermeldungen ausgegeben (siehe *Lizenzüberschreitung* auf Seite 34).

Für die Lizenzverwaltung bietet das SafeGuard Management Center im Bereich **Benutzer & Computer** einen Überblick zum Lizenzstatus des installierten SafeGuard Enterprise Systems. Der Lizenzstatusüberblick steht in der Registerkarte **Lizenzen** für den Stamm-Knoten, für Domänen, OUs, Containerobjekte und Arbeitsgruppen zur Verfügung. Sicherheitsbeauftragte erhalten hier detaillierte Informationen zum Lizenzstatus und können mit der entsprechenden Berechtigung Lizenzen in die SafeGuard Enterprise Datenbank importieren.

Dieses Kapitel beschreibt das Lizenzkonzept sowie die Verwaltung von Lizenzen im SafeGuard Management Center.

6.1 Lizenzdatei

Die Lizenzdatei, die Sie zum Import in die SafeGuard Enterprise Datenbank erhalten, ist eine .XML-Datei mit Signatur. Sie enthält folgende Informationen:

- Kundenname
- Zusätzliche Informationen (zum Beispiel Abteilung, Niederlassung)
- Datum, an dem die Lizenz ausgestellt wurde.
- Bereich von SafeGuard Enterprise Versionen, für den die Lizenz gültig ist.
- Anzahl an Lizenzen pro Modul
- Token-Lizenzinformationen
- Lizenzablaufdatum
- Lizenztyp (Demo- oder Voll-Lizenz)
- Signatur mit Lizenzsignaturzertifikat

6.2 Token-Lizenzen

Für die Verwaltung von Token bzw. Smartcards sind die entsprechenden zusätzlichen Token-Lizenzen erforderlich. Sind diese Token-Lizenzen nicht vorhanden, so lassen sich im SafeGuard Management Center keine Richtlinien für Token erstellen.

6.3 Evaluierungs- und Demo-Lizenzen

Es besteht die Möglichkeit, für Evaluierungs- oder initiale Rollout-Prozesse die Standard-Lizenzdatei (Evaluierungslizenz) oder individuelle Demo-Lizenzdateien zu nutzen. Die Nutzungsdauer dieser Lizenzen ist zeitlich begrenzt, die Funktionalität ist jedoch in keinster Weise eingeschränkt.

Hinweis: Evaluierungs- und Demo-Lizenzen dürfen nicht für den regulären produktiven Betrieb von SafeGuard Enterprise Modulen genutzt werden.

6.3.1 Standard-Lizenzdatei

Bei der Installation des SafeGuard Management Centers wird automatisch eine Standard-Lizenzdatei geladen. Diese Evaluierungslizenz mit der Bezeichnung SafeGuard Enterprise Evaluation License enthält jeweils fünf Lizenzen pro Modul und hat eine zeitlich begrenzte Gültigkeitsdauer von zwei Jahren ab dem Release-Datum der jeweiligen SafeGuard Enterprise Version.

6.3.2 Individuelle Demo-Lizenzdateien

Sollte die Standard-Lizenzdatei für die Durchführung einer Evaluierung nicht ausreichen, so besteht auch die Möglichkeit, eine an Ihre spezifischen Anforderungen angepasste Demo-Lizenz zu erhalten. Wenden Sie sich hierzu bitte an Ihren Vertriebspartner. Die Nutzungsdauer einer solchen Demo-Lizenz ist ebenfalls zeitlich begrenzt. Darüber hinaus ist die Lizenz auf die jeweils mit dem Vertriebspartner vereinbarte Anzahl an Lizenzen pro Modul beschränkt.

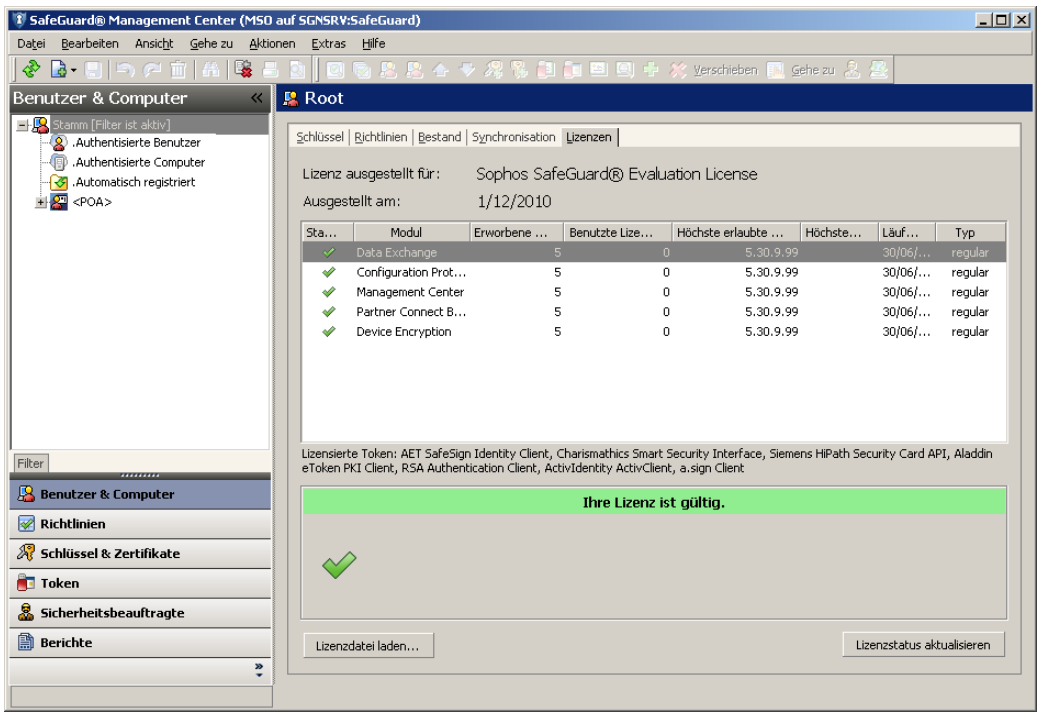
Wenn Sie das SafeGuard Management Center starten, werden Sie durch eine Warnungsmeldung darauf aufmerksam gemacht, dass Sie Demo-Lizenzen nutzen. Bei Überschreiten der in einer Demo-Lizenz festgelegten Anzahl an verfügbaren Lizenzen oder der zeitlich begrenzten Nutzungsdauer wird eine Fehlermeldung ausgegeben, siehe *Lizenzüberschreitung* auf Seite 34.

6.4 Lizenzstatusüberblick

So rufen Sie den Lizenzstatusüberblick auf:

1. Sie befinden sich im geöffneten Management Center im Bereich **Benutzer & Computer**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf den Stammknoten, die Domäne, die OU, das Containerobjekt oder die Arbeitsgruppe.
3. Wechseln Sie im Aktionsbereich auf der rechten Seite in die Registerkarte **Lizenzen**.

Der Lizenzstatus wird angezeigt.


SafeGuard® Management Center (MSO auf SGNSRV:SafeGuard)
Datei Bearbeiten Ansicht Gehe zu Aktionen Extras Hilfe
Verschieben Gehe zu
Benutzer & Computer
Stamm [Filter ist aktiv]
.Authentisierte Benutzer
.Authentisierte Computer
.Automatisch registriert
<POA>
Filter
Benutzer & Computer
Richtlinien
Schlüssel & Zertifikate
Token
Sicherheitsbeauftragte
Berichte
Root
Schlüssel Richtlinien Bestand Synchronisation Lizenzen
Lizenz ausgestellt für: Sophos SafeGuard® Evaluation License
Ausgestellt am: 1/12/2010
Sta... Modul Erworbene ... Benutzte Lize... Höchste erlaubte ... Höchste... Läuf... Typ
Data Exchange 5 0 5.30.9.99 30/06/... regular
Configuration Prot... 5 0 5.30.9.99 30/06/... regular
Management Center 5 0 5.30.9.99 30/06/... regular
Partner Connect B... 5 0 5.30.9.99 30/06/... regular
Device Encryption 5 0 5.30.9.99 30/06/... regular
Lizensierte Token: AET SafeSign Identity Client, Charismathics Smart Security Interface, Siemens HiPath Security Card API, Aladdin eToken PKI Client, RSA Authentication Client, ActivIdentity ActivClient, a.sign Client
Ihre Lizenz ist gültig.
Lizenzdatei laden...
Lizenzstatus aktualisieren

Die Anzeige ist in drei Bereiche unterteilt. Der obere Bereich zeigt den Namen des Kunden, für den die Lizenz ausgestellt wurde, sowie das Datum, an dem die Lizenz ausgestellt wurde.

Der mittlere Bereich liefert detaillierte Informationen zur Lizenz. Die einzelnen Spalten enthalten folgende Angaben:

Spalte	Erklärung
Status (Symbol)	Zeigt den Status der Lizenzen (gültig, Warnung, Fehler) für das jeweilige Modul durch ein Symbol an.
Modul	Zeigt das installierte Modul an.
Erworbene Lizenzen	Zeigt die Anzahl an erworbenen Lizenzen für das installierte Modul an.
Benutzte Lizenzen	Zeigt die Anzahl an genutzten Lizenzen für das installierte Modul an.
Höchste erlaubte Version	Zeigt die höchste SafeGuard Enterprise Version, für die die Lizenzen gültig sind, an.
Höchste benutzte Version	Zeigt die neueste installierte SafeGuard Enterprise Version an.
Läuft ab	Zeigt das Lizenzablaufdatum an.
Typ	Gibt die Lizenzart, Demo-Lizenz oder reguläre Voll-Lizenz, an.
Toleranzwert	Zeigt den festgelegten Toleranzwert für die Überschreitung der Anzahl an erworbenen Lizenzen an.

Wenn Sie die Registerkarte **Lizenzen** in einer Domäne/OU aufrufen, zeigt die Übersicht den Status basierend auf den Computern im jeweiligen Zweig.

Unterhalb dieser Übersicht finden Sie Informationen zu den lizenzierten Token-Modulen.

Im unteren Bereich wird der globale Lizenzstatus unabhängig davon, welche Domäne oder OU ausgewählt wurde, angezeigt. Dies erfolgt durch eine Meldung mit einer dem Ampelprinzip folgenden Hintergrundfarbe (Grün = gültig, Gelb = Warnung, Rot = Fehler) und ein Symbol. Bei Warnungs- und Fehlermeldungen erhalten Sie außerdem im unteren Bereich Hinweise zur Aufhebung des ungültigen Lizenzstatus.

Die im mittleren und unteren Bereich angezeigten Symbole haben folgende Bedeutung:

Gültige Lizenz

Ungültige Lizenz: Warnung

Ungültige Lizenz: Fehler

Zu Lizenzstatus, die eine Warnung oder einen Fehler zur Folge haben, siehe *Lizenzüberschreitung* auf Seite 34.

Sie können die Ansicht des Lizenzstatusüberblicks aktualisieren, indem Sie auf die Schaltfläche **Lizenzstatus aktualisieren** klicken.

6.5 Lizenzdateien importieren

Voraussetzung: Um eine Lizenzdatei in die SafeGuard Enterprise Datenbank zu importieren, benötigen Sie als Sicherheitsbeauftragter die Berechtigung „Lizenzdatei importieren“.

So importieren Sie eine Lizenzdatei:

1. Sie befinden sich im geöffneten Management Center im Bereich **Benutzer & Computer**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf den Stamm-Knoten, die Domäne oder die OU.
3. Wechseln Sie im Aktionsbereich auf der rechten Seite in die Registerkarte **Lizenzen**.
4. Klicken Sie auf die Schaltfläche **Lizenzdatei importieren**. Es wird ein Fenster zur Auswahl der Lizenzdatei angezeigt.
5. Wählen Sie die zu importierende Lizenzdatei aus und klicken Sie auf **Öffnen**.
6. Der Inhalt der neuen Lizenzdatei wird im Überblick angezeigt. Bestätigen Sie, dass Sie die Lizenzdatei importieren möchten.

Die Lizenzdatei wurde in die SafeGuard Enterprise Datenbank importiert.

Nach dem Import der Lizenzdatei wird bei Modulen, für die Lizenzen erworben wurden, der Lizenztyp **regulär** angegeben. Bei Modulen, für die keine Lizenzen erworben wurden und für die die Evaluierungslizenz (Standard-Lizenzdatei) oder individuelle Demo-Lizenzen für Evaluierungsprozesse genutzt werden, wird der Lizenztyp **Demo** angegeben.

Hinweis: Wenn Sie eine neue Lizenzdatei importieren, werden jeweils nur die Module, die in dieser Datei enthalten sind, aktualisiert. Alle übrigen Modul-Lizenzinformationen werden entsprechend den in der Datenbank enthaltenen Informationen beibehalten. Dieses Importverhalten vereinfacht die spätere Evaluierung von zusätzlichen Modulen, wenn Sie bereits ein oder mehrere Module erworben haben.

6.6 Lizenzüberschreitung

In Ihrer Lizenzdatei ist ein Toleranzwert für die Überschreitung der erworbenen Lizenzen sowie der Lizenzgültigkeitsdauer festgelegt. Bei Überschreiten der verfügbaren Lizenzen pro Modul oder der Gültigkeitsdauer wird somit zunächst eine Warnungsmeldung ausgegeben. Der laufende Betrieb des Systems wird dadurch nicht beeinträchtigt und es tritt in diesem Fall auch keine Einschränkung der Funktionalität in Kraft. So haben Sie die Gelegenheit, den Lizenzstatus zu prüfen und Ihre Lizenz zu erweitern bzw. zu erneuern. Der Toleranzwert ist auf 10 % der Anzahl an erworbenen Lizenzen (Mindestwert: 5, Höchstwert: 5.000) festgelegt.

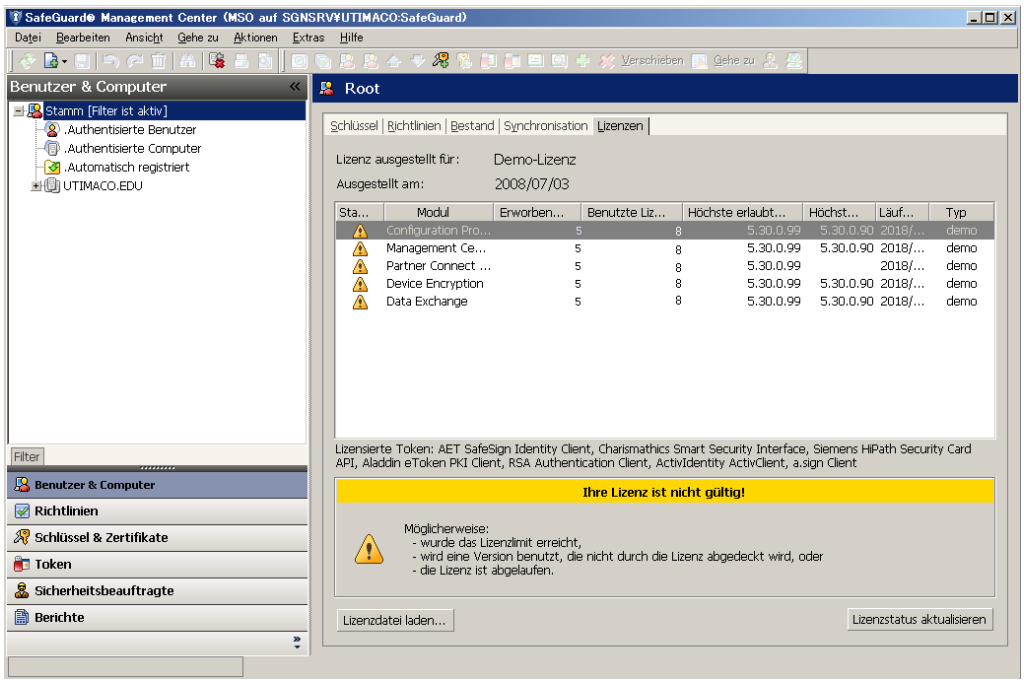
Bei Überschreiten der Toleranzwerte wird eine Fehlermeldung ausgegeben. In diesem Fall tritt eine Einschränkung der Funktionalität ein. Die Übertragung von Richtlinien an die Benutzer-Computer wird deaktiviert. Diese Deaktivierung lässt sich nicht im SafeGuard Management Center manuell wieder aufheben. Die Lizenz muss erweitert bzw. erneuert werden, um die Funktionalität wieder in vollem Umfang nutzen zu können. Außer der Deaktivierung der Richtlinienübertragung hat die Funktionalitätseinschränkung keine Auswirkungen auf die Benutzer-Computer, bereits zugeordnete Richtlinien bleiben aktiv. Darüber hinaus lassen sich auch bei Deaktivierung der Richtlinienübertragung Clients deinstallieren.

Die folgenden Abschnitte beschreiben das Systemverhalten bei Lizenzüberschreitungen der Kategorien Warnung und Fehler sowie die Maßnahmen zur Aufhebung der Funktionalitätseinschränkung.

6.6.1 Ungültige Lizenz: Warnung

Wird die Anzahl an verfügbaren Lizenzen, das Lizenzgültigkeitsdatum oder die höchste zulässige SafeGuard Enterprise Version (zum Beispiel durch ein Software-Update) überschritten, so wird beim Starten des SafeGuard Management Centers eine Warnungsmeldung angezeigt.

Das SafeGuard Management Center wird geöffnet und zeigt den Lizenzstatusüberblick in der Registerkarte **Lizenzen** des Bereichs **Benutzer & Computer**.


SafeGuard® Management Center (MSO auf SGNSRV¥UTIMACO:SafeGuard)
Datei Bearbeiten Ansicht Gehe zu Aktionen Extras Hilfe
Verschieben Gehe zu
Benutzer & Computer
Stamm [Filter ist aktiv]
.Authentisierte Benutzer
.Authentisierte Computer
.Automatisch registriert
UTIMACO.EDU
Filter
Benutzer & Computer
Richtlinien
Schlüssel & Zertifikate
Token
Sicherheitsbeauftragte
Berichte
Root
Schlüssel Richtlinien Bestand Synchronisation Lizenzen
Lizenz ausgestellt für: Demo-Lizenz
Ausgestellt am: 2008/07/03
Sta... Modul Erworben... Benutzte Liz... Höchste erlaubt... Höchst... Läuf... Typ
Configuration Pro... 5 8 5.30.0.99 5.30.0.90 2018/... demo
Management Ce... 5 8 5.30.0.99 5.30.0.90 2018/... demo
Partner Connect ... 5 8 5.30.0.99 2018/... demo
Device Encryption 5 8 5.30.0.99 5.30.0.90 2018/... demo
Data Exchange 5 8 5.30.0.99 5.30.0.90 2018/... demo
Lizensierte Token: AET SafeSign Identity Client, Charismathics Smart Security Interface, Siemens HiPath Security Card API, Aladdin eToken PKI Client, RSA Authentication Client, ActivIdentity ActivClient, a.sign Client
Ihre Lizenz ist nicht gültig!
Möglicherweise:
- wurde das Lizenzlimit erreicht,
- wird eine Version benutzt, die nicht durch die Lizenz abgedeckt wird, oder
- die Lizenz ist abgelaufen.
Lizenzdatei laden...
Lizenzstatus aktualisieren

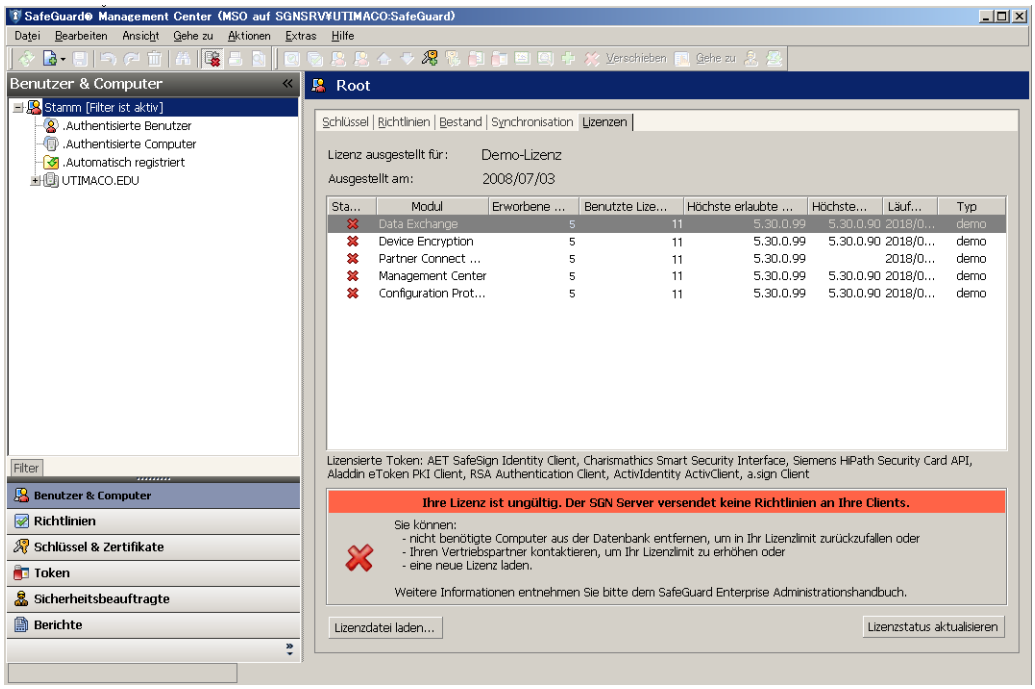
Auch hier informiert Sie eine Warnungsmeldung darüber, dass die Lizenz ungültig ist. Über die angezeigten detaillierten Informationen zur Lizenzdatei lässt sich ermitteln, für welches Modul die Anzahl an verfügbaren Lizenzen überschritten wurde. Durch Verlängerung, Erneuerung oder Erweiterung der Lizenz lässt sich dieser Lizenzstatus wieder aufheben, siehe *Ungültige Lizenz: Fehler* auf Seite 36.

6.6.2 Ungültige Lizenz: Fehler

Wird der in der Lizenz festgelegte Toleranzwert für die Anzahl an Lizenzen oder die Gültigkeitsdauer überschritten, so zeigt das SafeGuard Management Center eine Fehlermeldung an.

Im SafeGuard Management Center wird die Übertragung von Richtlinien auf die Benutzer-Computer deaktiviert.

In der Registerkarte **Lizenzen** im Bereich **Benutzer & Computer** wird ebenfalls eine Fehlermeldung angezeigt.


SafeGuard® Management Center (MSO auf SGNSRV\UTIMACO:SafeGuard)
Datei Bearbeiten Ansicht Gehe zu Aktionen Extras Hilfe
Verschieben Gehe zu
Benutzer & Computer
Stamm [Filter ist aktiv]
.Authentisierte Benutzer
.Authentisierte Computer
.Automatisch registriert
UTIMACO.EDU
Filter
Benutzer & Computer
Richtlinien
Schlüssel & Zertifikate
Token
Sicherheitsbeauftragte
Berichte
Root
Schlüssel Richtlinien Bestand Synchronisation Lizenzen
Lizenz ausgestellt für: Demo-Lizenz
Ausgestellt am: 2008/07/03
Sta... Modul Erworbene ... Benutzte Lize... Höchste erlaubte ... Höchste... Läuf... Typ
Data Exchange 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Device Encryption 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Partner Connect ... 5 11 5.30.0.99 2018/0... demo
Management Center 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Configuration Prot... 5 11 5.30.0.99 5.30.0.90 2018/0... demo
Lizensierte Token: AET SafeSign Identity Client, Charismathics Smart Security Interface, Siemens HiPath Security Card API, Aladdin eToken PKI Client, RSA Authentication Client, ActivIdentity ActivClient, a.sign Client
Ihre Lizenz ist ungültig. Der SGN Server versendet keine Richtlinien an Ihre Clients.
Sie können:
- nicht benötigte Computer aus der Datenbank entfernen, um in Ihr Lizenzlimit zurückzufallen oder
- Ihren Vertriebspartner kontaktieren, um Ihr Lizenzlimit zu erhöhen oder
- eine neue Lizenz laden.
Weitere Informationen entnehmen Sie bitte dem SafeGuard Enterprise Administrationshandbuch.
Lizenzdatei laden...
Lizenzstatus aktualisieren

Über die detaillierten Informationen zur Lizenzdatei lässt sich ermitteln, für welches Modul die Anzahl an verfügbaren Lizenzen überschritten wurde.

Zur Aufhebung der Funktionalitätseinschränkung haben Sie folgende Möglichkeiten:

- Lizenzen umverteilen

  Um wieder ausreichend verfügbare Lizenzen zu erhalten, können Sie die Software auf nicht genutzten Computern deinstallieren und somit die Computer dauerhaft aus der SafeGuard Enterprise Datenbank entfernen.

- Lizenzen erweitern/erneuern

  Wenden Sie sich an Ihren Vertriebspartner, um Ihre Lizenz zu erweitern bzw. zu erneuern. Sie erhalten eine neue Lizenzdatei zum Import in die SafeGuard Enterprise Datenbank.

- Neue Lizenzdatei importieren

  Wenn Sie Ihre Lizenz bereits erneuert bzw. erweitert haben, importieren Sie die erhaltene Lizenzdatei in die SafeGuard Enterprise Datenbank. Die neu importierte Datei ersetzt die ungültige Lizenzdatei.

Durch Umverteilen von Lizenzen oder Importieren einer gültigen Lizenzdatei wird die Funktionalitätseinschränkung aufgehoben und der normale Betrieb des Systems kann fortgesetzt werden.

7 SafeGuard Enterprise Sicherheitsbeauftragte

SafeGuard Enterprise kann von einem oder mehreren Sicherheitsbeauftragten administriert werden. Mit der rollenbasierten Administration ist es möglich, die Verwaltung von SafeGuard Enterprise auf mehrere Benutzer zu verteilen. Dabei kann einem Benutzer eine oder mehrere Rollen zugewiesen werden. Um die Sicherheit noch zu erhöhen, kann einer Sicherheitsbeauftragtenrolle die zusätzliche Autorisierung eines Vorgangs zugewiesen werden.

Während der initialen Konfiguration des SafeGuard Management Center wird automatisch ein Administrator höchster Ebene angelegt: der Haupt-Sicherheitsbeauftragte (Master Security Officer, MSO). Dieser verfügt über alle Rechte sowie über ein Zertifikat, das nicht abläuft. Für andere spezifische Aufgaben, z. B. Helpdesk- oder Audit-Aufgaben, können dann weitere Sicherheitsbeauftragte zugewiesen werden.

Sicherheitsbeauftragte lassen sich im Navigationsbereich des SafeGuard Management Center gemäß der Organisationsstruktur Ihres Unternehmens hierarchisch anordnen. Diese hierarchische Anordnung gibt jedoch keine Hierarchie in Bezug auf Rechte und Rollen wieder.

7.1 Rollen für Sicherheitsbeauftragte

SafeGuard Enterprise bietet für die komfortable Verwaltung bereits vordefinierte Rollen mit verschiedenen Funktionen für Sicherheitsbeauftragte an. Darüber hinaus hat ein Sicherheitsbeauftragter mit den erforderlichen Rechten die Möglichkeit, aus einer Liste von Aktionen/Rechten selbst neue Rollen zu definieren und bestimmten Sicherheitsbeauftragten zuzuweisen.

Folgende Rollentypen stehen zur Verfügung:

- Rolle des Haupt-Sicherheitsbeauftragten (Master Security Officer, MSO)
- Vordefinierte Rollen
- Benutzerdefinierte Rollen

7.1.1 Haupt-Sicherheitsbeauftragter

Nach der Installation von SafeGuard Enterprise wird bei der initialen Konfiguration des SafeGuard Management Center automatisch ein Haupt-Sicherheitsbeauftragter (Master Security Officer, MSO) angelegt. Der Haupt-Sicherheitsbeauftragte ist der Sicherheitsbeauftragte der höchsten Ebene und hat alle Rechte sowie Zugriff auf alle Objekte, vergleichbar mit dem Administrator bei Windows. Die Rechte des Haupt-Sicherheitsbeauftragten können nicht geändert werden.

Für eine Instanz des SafeGuard Management Centers können mehrere Haupt-Sicherheitsbeauftragte angelegt werden. Aus Sicherheitsgründen empfehlen wir, mindestens einen weiteren Haupt-Sicherheitsbeauftragten anzulegen. Zusätzliche Haupt-Sicherheitsbeauftragte können jederzeit gelöscht werden, es muss jedoch immer ein Benutzer mit der Rolle des Haupt-Sicherheitsbeauftragten vorhanden sein, der explizit als Hauptsicherheits-Beauftragter in der SafeGuard Enterprise Datenbank angelegt wurde.

Ein Haupt-Sicherheitsbeauftragter kann Aufgaben an andere Personen delegieren. Dazu gibt es zwei Möglichkeiten:

- Ein neuer Benutzer/Sicherheitsbeauftragter kann unter **Sicherheitsbeauftragte** angelegt werden.
- Ein aus dem Active Directory importierter und im Stammverzeichnis des Management Center sichtbarer Benutzer oder alle Mitglieder eines Containers können unter **Benutzer & Computer** zu Sicherheitsbeauftragten gemacht werden.

Den Sicherheitsbeauftragten können eine oder mehrere Rollen zugeordnet werden. Einem Benutzer kann z. B. die Rolle des Verwaltungsbeauftragten und die Rolle des Helpdesk-Beauftragten zugewiesen werden.

Hinweis: Der Haupt-Sicherheitsbeauftragte kann aber auch selbst definierte Rollen anlegen und bestimmten Sicherheitsbeauftragten zuweisen.

7.1.2 Vordefinierte Rollen

Im SafeGuard Management Center sind neben dem Haupt-Sicherheitsbeauftragten die folgenden Rollen vordefiniert. Die diesen vordefinierten Rollen zugewiesenen Rechte können nicht geändert werden. Verfügt eine vordefinierte Rolle z. B. über das Recht „Richtlinien und Richtliniengruppen anlegen“, so kann dieses Recht nicht aus der Rolle entfernt werden.
Es können auch keine neuen Rechte zu einer vordefinierten Rollen hinzugefügt werden.
Die zusätzliche Autorisierung durch einen weiteren Sicherheitsbeauftragten hingegen lässt sich jederzeit den vordefinierten Rollen zuordnen.

- **Verwaltungsbeauftragter**

  Verwaltungsbeauftragte können Ihren eigenen Knoten im Bereich Sicherheitsbeauftragte einsehen und sind dazu berechtigt, die ihrem Knoten zugehörigen Sicherheitsbeauftragten zu verwalten.

- **Sicherheitsbeauftragter**

  Sicherheitsbeauftragte haben umfassende Rechte u. a. für die SafeGuard Enterprise Konfiguration, Richtlinien- und Schlüsselverwaltung sowie für Überwachung und Recovery.

- **Helpdesk-Beauftragter**

  Helpdesk-Beauftragte sind zurDurchführung von Recovery-Vorgängen berechtigt. Darüber hinaus können Sie sich die meisten Funktionsbereiche des SafeGuard Management Center anzeigen lassen.

- **Audit-Beauftragter**

  Um SafeGuard Enterprise überwachen zu können, haben Audit-Beauftragte die Berechtigung, sich die meisten Funktionsbereiche des SafeGuard Management Center anzeigen zu lassen.

- **Recovery-Beauftragter**

  Recovery-Beauftragte sind dazu berechtigt, die SafeGuard Enterprise Datenbank zu reparieren.

7.1.3 Benutzerdefinierte Rollen

Als Sicherheitsbeauftragter mit den erforderlichen Rechten können Sie neue Rollen aus einer Liste mit Aktionen/Rechten definieren und sie einem vorhandenen oder einem neuen Sicherheitsbeauftragten zuweisen. Wie auch bei den vordefinierten Rollen lässt sich die zusätzliche Autorisierung durch einen weiteren Sicherheitsbeauftragten für eine Funktion der betreffenden Rolle jederzeit aktivieren.

Bei der Zuweisung einer neuen Rolle ist für die zusätzliche Autorisierung Folgendes zu beachten:

Achtung: Wenn ein Benutzer zwei Rollen mit der gleichen Funktion inne hat, und bei einer der Rollen die zusätzliche Autorisierung zugeordnet ist, dann gilt das automatisch auch bei der anderen Rolle.

Ein Sicherheitsbeauftragter mit den erforderlichen Rechten kann Rechte zu einer benutzerdefinierten Rolle hinzufügen oder Rechte aus der Rolle entfernen. Im Gegensatz zu vordefinierten Rollen können benutzerdefinierte je nach Anforderung auch gelöscht werden. Ist einem Benutzer nur eine Rolle zugewiesen und wird diese Rolle gelöscht. so kann sich der Benutzer nicht mehr am SafeGuard Management Center anmelden.

Die Rolle und die darin definierten Aktionen bestimmen, was ein Benutzer darf und was nicht. Auch dann, wenn dem Benutzer mehrere Rollen zugewiesen worden sind. Nachdem er sich am System angemeldet hat, werden nur die Bereiche des Management Centers aktiviert und angezeigt, die für seine Rolle nötig sind. Das betrifft auch die Bereiche Skripte und API.
Sie sollten deshalb für einen Bereich, in dem Sie Aktionen vergeben, immer auch die Anzeige dieses Bereichs als Aktion auswählen. Aktionen werden nach Funktionsbereich sortiert und sind hierarchisch strukturiert. Diese Struktur zeigt, welche Aktionen vor der Durchführung bestimmter anderer Aktionen erforderlich sind.

7.1.4 Zusätzliche Autorisierung

Die zusätzliche Autorisierung (auch Vier-Augen-Prinzip genannt) kann spezifischen Aktionen einer Rolle zugeordnet werden. Das bedeutet, dass der Benutzer dieser Rolle eine bestimmte Aktion nur ausführen darf, wenn ein Benutzer einer weiteren Rolle anwesend ist und die Ausführung der Aktion bestätigt.

Die zusätzliche Autorisierung lässt sich sowohl vordefinierten als auch benutzerdefinierten Rollen zuweisen. Sobald es mindestens zwei Beauftragte mit der gleichen Rolle gibt, kann auch die eigene Rolle ausgewählt werden.

Die Rolle, die die zusätzliche Autorisierung durchführen soll, muss einem Benutzer zugewiesen sein und es müssen mindestens zwei Benutzer in der SafeGuard Datenbank vorhanden sein. Wenn die zusätzliche Autorisierung für eine Aktion erforderlich ist, ist sie auch dann erforderlich, wenn der Benutzer eine weitere Rolle hat, die die zusätzliche Autorisierung für diese Aktion nicht erfordert.

Wenn ein Sicherheitsbeauftragter ohne Berechtigung zum Ändern der Einstellungen für die zusätzliche Autorisierung eine Rolle anlegt, werden die Einstellungen für die zusätzliche Autorisierung der neuen Rolle gemäß den definierten Einstellungen für den anlegenden Benutzer voreingestellt.

Hinweis: Zwei Sicherheitsbeauftragte dürfen auf einem Computer nicht dasselbe Windows Account benutzern. Andernfalls lassen sich ihre Zugriffsrechte nicht sauber trennen. Unter Umständen ist die zusätzliche Autorisierung nur dann sinnvoll, wenn sich die Sicherheitsbeauftragten über kryptographische Token/Smartcards anmelden müssen.

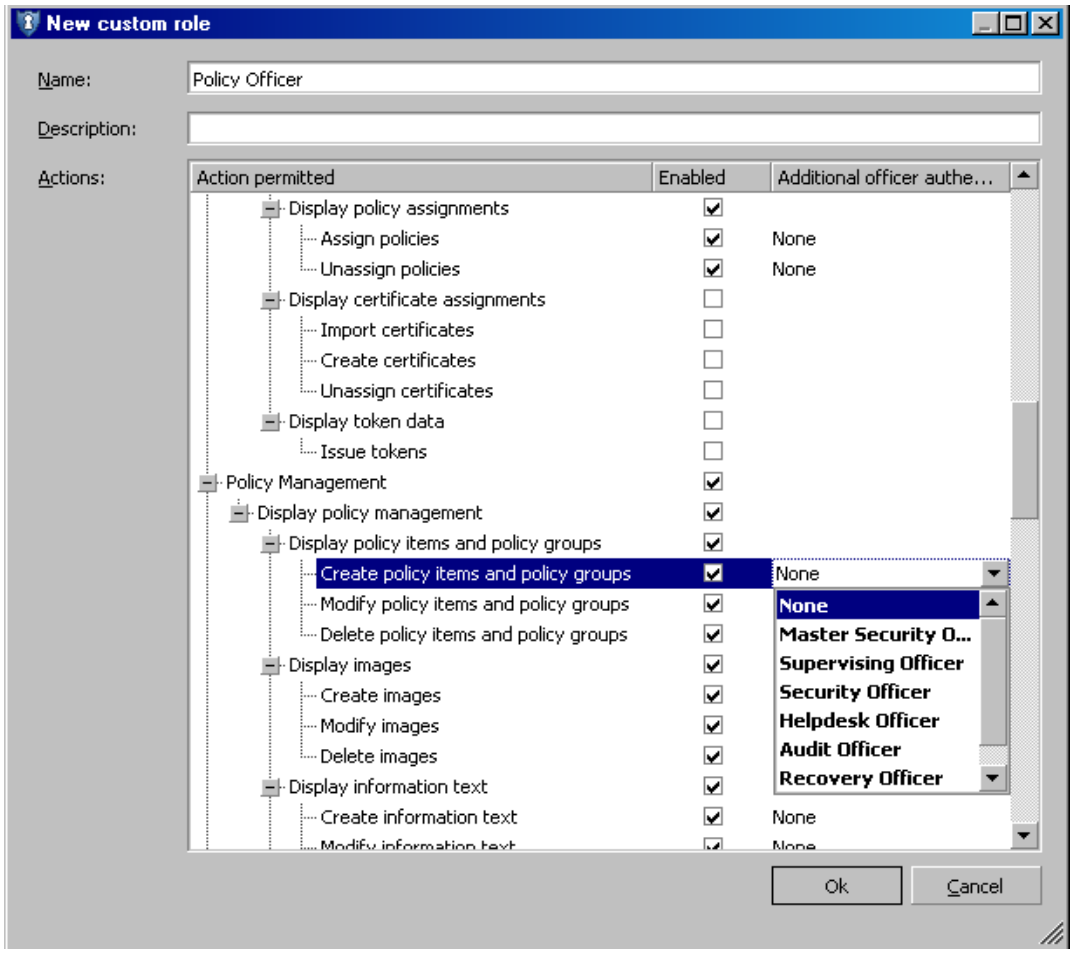
7.2 Eine neue Rolle anlegen

Voraussetzung: Um eine neue Rolle anzulegen, benötigen Sie das Recht, benutzerdefinierte Rollen einzusehen und zu verwalten. Um die zusätzliche Autorisierung zuzuweisen, benötigen Sie das Recht „Einstellungen für zusätzliche Autorisierung ändern“.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie mit der rechten Maustaste auf **Benutzerdefinierte Rollen** und wählen Sie **Neu > Neue benutzerdefinierte Rolle**.
3. Geben Sie im Dialog **Neue benutzerdefinierte Rolle** einen Namen und eine Beschreibung für die Rolle ein.
4. Wählen Sie die Aktionen für diese Rolle: Aktivieren Sie die Kontrollkästchen neben den gewünschten Aktionen in der Spalte **Aktiv**. Die Aktionen sind nach Funktionsbereich sortiert und hierarchisch strukturiert. Diese Struktur zeigt, welche Aktionen vor der Durchführung bestimmter anderer Aktionen erforderlich sind.
5. Falls erforderlich, weisen Sie die **zusätzliche Autorisierung** zu: Klicken Sie auf die Standardeinstellung **Kein** und wählen Sie die gewünschte Rolle aus der angezeigten Dropdownliste. Wenn ein Sicherheitsbeauftragter ohne die Berechtigung zum Ändern der zusätzlichen Autorisierung eine Rolle anlegt, wird die zusätzliche Autorisierung gemäß den Einstellungen der Rolle des betreffenden Sicherheitsbeauftragten vordefiniert. Die zusätzliche Autorisierung kann ausgewählt werden, wenn sie für mehr als eine Rolle des Sicherheitsbeauftragten eingestellt ist.
6. Klicken Sie auf **OK**.

Die neue Rolle wird unter **Benutzerdefinierte Rollen** im Navigationsfenster angezeigt. Wenn Sie die Rolle anklicken, werden im rechten Aktionsbereich die zulässigen Aktionen dargestellt.



7.3 Rolle einem Sicherheitsbeauftragten zuweisen

Voraussetzung: Um eine neue Rolle anzulegen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu ändern.

Gehen Sie wie folgt vor:

1. Wählen Sie den gewünschten Sicherheitsbeauftragten im Navigationsfenster aus. Die Eigenschaften werden im rechten Aktionsbereich für ihn angezeigt.
2. Weisen Sie die gewünschten Rollen durch Aktivieren der entsprechenden Kontrollkästchen zu. Vordefinierte Rollen werden fett angezeigt.
3. Klicken Sie auf das Doppelpfeil-Symbol **Aktualisieren** in der Symbolleiste.

Die Rolle ist dem Sicherheitsbeauftragten nun zugewiesen.

7.4 Sicherheitsbeauftragten- und Rolleneigenschaften einsehen

Voraussetzung: Um sich einen Überblick über die Sicherheitsbeauftragteneigenschaften oder die Rollenzuordnungen anzeigen zu lassen, benötigen Sie das Recht zum Einsehen von Sicherheitsbeauftragten und Sicherheitsbeauftragtenrollen.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Doppelklicken Sie im Navigationsbereich auf der linken Seite auf dem Objekt, zu dem Sie einen Überblick erhalten möchten.

Die im Aktionsbereich angezeigten Informationen richten sich nach dem ausgewählten Objekt.

7.4.1 Eigenschaften für den Haupt-Sicherheitsbeauftragten anzeigen

Die allgemeinen Informationen sowie die Änderungsinformationen für den Haupt-Sicherheitsbeauftragten werden angezeigt.

7.4.2 Eigenschaften für Sicherheitsbeauftragte anzeigen

Die allgemeinen Informationen sowie die Änderungsinformationen für den Sicherheitsbeauftragten werden angezeigt.

1. Wählen Sie unter **Eigenschaften** die Registerkarte **Aktionen**. Diese Registerkarte bietet eine Zusammenfassung der zulässigen Aktionen sowie der Rollen, die dem Sicherheitsbeauftragten zugewiesen sind.

7.4.3 Rechte und Rollen von Sicherheitsbeauftragten anzeigen

Eine Zusammenfassung der Aktionen aller Rollen, die dem Sicherheitsbeauftragten zugewiesen sind, wird angezeigt. Die Baumstrukturansicht zeigt, welche Aktionen erforderlich sind, damit bestimmte andere Aktionen durchgeführt werden können. Darüber hinaus können die zugewiesenen Rollen angezeigt werden.

1. Wählen Sie unter **Aktionen** eine Aktion, um alle zugewiesenen Rollen anzeigen zu lassen, die diese Aktion enthalten.

2. Doppelklicken Sie auf einer Rolle, um den Dialog **Eigenschaften** zu schließen und danach die Eigenschaften der Rolle anzeigen zu lassen.

7.4.4 Rolleneigenschaften anzeigen

Die allgemeinen Informationen sowie die Änderungsinformationen für die Rolle werden angezeigt.

1. Wählen Sie unter **Eigenschaften** die Registerkarte **Zuweisung**, um die Sicherheitsbeauftragten anzeigen zu lassen, die dieser Rolle zugeordnet sind.

7.4.5 Rollenzuordnung anzeigen

Doppelklicken Sie unter **Zuweisung** auf einem Sicherheitsbeauftragten, um den Dialog **Eigenschaften** zu schließen und danach die allgemeinen Daten und Rollen des Sicherheitsbeauftragten anzeigen zu lassen.

7.5 Rolle ändern

Für das Ändern von Rollen gibt es folgende Möglichkeiten:

- Sie können nur die Einstellungen für die zusätzliche Autorisierung ändern.
- Sie können alle Eigenschaften der Rolle ändern.

Das Symbol neben den Rollen zeigt, welche Aktion möglich ist:

Symbol	Beschreibung
	Die Rolle kann geändert werden (Aktionen hinzufügen/löschen).
	Die zusätzliche Autorisierung kann geändert werden.
	Beide Änderungsmöglichkeiten sind verfügbar.

Hinweis: Vordefinierte Rollen und die ihnen zugewiesenen Aktionen können nicht geändert werden. Ist die zusätzliche Autorisierung aktiviert, so kann dies für jede Rolle, auch für vordefinierte Rollen, geändert werden.

7.5.1 Zusätzliche Autorisierung ändern

Voraussetzung: Um die zusätzliche Autorisierung zuzuweisen, benötigen Sie das Recht, Sicherheitsbeauftragtenrollen einzusehen sowie das Recht „Einstellungen für zusätzliche Autorisierung ändern“.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster unter **Benutzerdefinierte Rollen** auf die Rolle, die Sie ändern möchten. Klicken Sie im Aktionsbereich auf der rechten Seite bei der gewünschten Einstellung in der Spalte **Zusätzliche Autorisierung** und wählen Sie eine andere Rolle aus der Liste aus. Vordefinierte Rollen werden fett angezeigt.
3. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die zusätzliche Autorisierung für diese Rolle wurde geändert.

7.5.2 Alle Eigenschaften einer Rolle ändern

Voraussetzung: Um eine benutzerdefinierte Rolle zu ändern, benötigen Sie das Recht zum Einsehen und Ändern von Sicherheitsbeauftragtenrollen. Zum Ändern der Einstellung für die zusätzliche Autorisierung benötigen Sie außerdem das Recht „Einstellungen für zusätzliche Autorisierung ändern“.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster unter **Benutzerdefinierte Rollen** auf die Rolle, die Sie ändern möchten, und wählen Sie **Sicherheitsbeauftragtenrolle ändern**.
3. Ändern Sie die Eigenschaften nach Wunsch. Ändern Sie die Einstellungen für die zusätzliche Autorisierung, indem Sie auf den Wert in dieser Spalte klicken und die gewünschte Rolle auswählen.
4. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die Rolle wurde geändert.

7.6 Rolle kopieren

Um eine Rolle anzulegen, die ähnliche Eigenschaften wie eine bereits vorhandene Rolle hat, können Sie die vorhandene Rolle als Vorlage benutzen. Sie können eine vordefinierte oder eine benutzerdefinierte Rolle als Vorlage auswählen.

Voraussetzung: Die Verwendung von vorhandenen Rollen als Vorlage ist nur dann möglich, wenn der derzeit authentisierte Sicherheitsbeauftragte alle Rechte hat, die in dieser spezifischen Rollenvorlage enthalten sind. Diese Funktion ist also u. U. für Sicherheitsbeauftragte, deren zulässige Aktionen begrenzt sind, nicht verfügbar.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf die Rolle, die Sie kopieren möchten, und wählen Sie **Neu > Neue Kopie der Rolle**. Unter **Neue benutzerdefinierte Rolle** werden alle Eigenschaften der vorhandenen Rolle bereits vorausgewählt.
3. Geben Sie einen neuen Namen für diese Rolle ein und ändern Sie die Eigenschaften nach Wunsch.
4. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die neue Rolle ist angelegt.

7.7 Rolle löschen

Hinweis: Vordefinierte Rollen können nicht gelöscht werden.

Voraussetzung: Um eine Rolle zu löschen, benötigen Sie das Recht zum Einsehen und Löschen von Sicherheitsbeauftragtenrollen.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster unter **Benutzerdefinierte Rollen** mit der rechten Maustaste auf die Rolle, die Sie löschen möchten, und wählen Sie **Löschen**. Je nach den Eigenschaften der Rolle wird eine entsprechende Warnungsmeldung angezeigt.

Hinweis: Wenn Sie eine Rolle löschen, geht diese Rolle bei allen Sicherheitsbeauftragten, denen sie zugeordnet ist, verloren. Ist einem Sicherheitsbeauftragten nur diese eine Rolle zugewiesen, so kann dieser sich erst wieder am SafeGuard Management Center anmelden, wenn ein übergeordneter Sicherheitsbeauftragter ihm eine neue Rolle zuweist. Wird die Rolle für die zusätzliche Autorisierung verwendet, so wird der Haupt-Sicherheitsbeauftragte dazu aufgefordert, die zusätzliche Autorisierung durchzuführen.

3. Um die Rolle zu löschen, bestätigen Sie die Meldung mit **Ja**.
4. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die Rolle wird aus dem Navigationsfenster entfernt und aus der Datenbank gelöscht.

7.8 Haupt-Sicherheitsbeauftragten anlegen

Voraussetzung: Um einen neuen Haupt-Sicherheitsbeauftragten anzulegen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und anzulegen.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Knoten **Haupt-Sicherheitsbeauftragte** und wählen Sie **Neu > Neuer Sicherheitsbeauftragter**.
3. Nehmen Sie die relevanten Einträge unter **Neuer Haupt-Sicherheitsbeauftragter** vor:

Eingabefeld/Kontrollkästchen	Beschreibung
Aktiviert	Hier kann der Beauftragte bis auf Weiteres deaktiviert werden. Das bedeutet, dass er zwar im System existiert, sich aber noch nicht an das SafeGuard Management Center anmelden kann. Erst wenn er durch einen anderen Beauftragten aktiviert wird, kann er sich anmelden und seine administrativen Tätigkeiten ausführen.
Kurzname	Hier wird der Name des Beauftragten angegeben, wie er in den von SafeGuard Enterprise erzeugten Zertifikaten unter cn= eingetragen wird. Unter diesem Namen wird er auch im Navigationsfenster des Management Centers angezeigt. Dieser Name muss eindeutig sein. Maximalwert: 256 Zeichen

Eingabefeld/Kontrollkästchen	Beschreibung
Beschreibung	Optional Maximalwert: 256 Zeichen
Mobiltelefon	Optional Maximalwert: 128 Zeichen
E-Mail	Optional Maximalwert: 256 Zeichen
Gültig ab/bis	Hier wird angegeben, ab und bis wann (Datum) sich der Beauftragte am Management Center anmelden darf.
Token-Anmeldung	Die Anmeldung kann auf folgende Art erfolgen: **Ohne Token** Der Sicherheitsbeauftragte darf sich nicht mit einem Token anmelden. Er muss sich über die Anmeldeinformationen (Benutzername/Kennwort) anmelden. **Optional** Die Anmeldung kann mit Token oder mit Anmeldeinformationen erfolgen. Der Sicherheitsbeauftragte kann wählen. **Zwingend erforderlich** Die Verwendung eines Token zur Anmeldung ist zwingend vorgeschrieben. Dazu muss sich der zum Zertifikat des Sicherheitsbeauftragten gehörende private Schlüssel auf dem Token befinden.

Eingabefeld/Kontrollkästchen	Beschreibung
Zertifikat	Zur Anmeldung an das Management Center benötigt ein Beauftragter immer ein Zertifikat. Das Zertifikat kann entweder von SafeGuard Enterprise selbst erstellt werden oder es wird ein bereits existierendes verwendet. Ist eine Anmeldung mit Token zwingend notwendig, so muss das Zertifikat auf den Token des Sicherheitsbeauftragten aufgebracht werden. **Erzeugen:** Zertifikat und Schlüsseldatei werden neu erstellt und an einem auswählbaren Ort gespeichert. Dabei muss ein Kennwort für die .p12-Schlüsseldatei angegeben und bestätigt werden. Die .p12-Datei muss dem Sicherheitsbeauftragten bei der Anmeldung zur Verfügung stehen. Das erstellte Zertifikat wird dem Sicherheitsbeauftragten automatisch zugeteilt und unter **Zertifikat** angezeigt. Wenn SafeGuard Enterprise Kennwortregeln angewendet werden, sollten die Regeln im Active Directory deaktiviert werden. **Hinweis:** Maximale Länge des Speicherpfads und des Dateinamens: 260 Zeichen. Zum Anlegen eines Sicherheitsbeauftragten ist der öffentliche Teil des Zertifikats zwar ausreichend. Bei der Anmeldung am Management Center wird allerdings der private Teil des Zertifikats, die Schlüsseldatei, verlangt. Liegt diese nicht in der Datenbank vor, muss sie dem Sicherheitsbeauftragten zur Verfügung stehen und kann bei der Anmeldung dann ggf. im Zertifikatsspeicher abgelegt werden.
Zertifikat	**Importieren:** Ein existierendes Zertifikat wird importiert und anschließend dem Beauftragten zugewiesen. Wird aus einer .p12 Schlüsseldatei importiert, muss das Kennwort des Zertifikats bekannt sein. Wird ein PKCS#12 Zertifikatscontainer ausgewählt, werden alle Zertifikate in die Liste der zuweisbaren Zertifikate geladen. Die Zuweisung des Zertifikats erfolgt nach dem Import, indem das Zertifikat im Dropdown-Listenfeld ausgewählt wird.

4. Klicken Sie zur Bestätigung Ihrer Einstellungen auf **OK**.

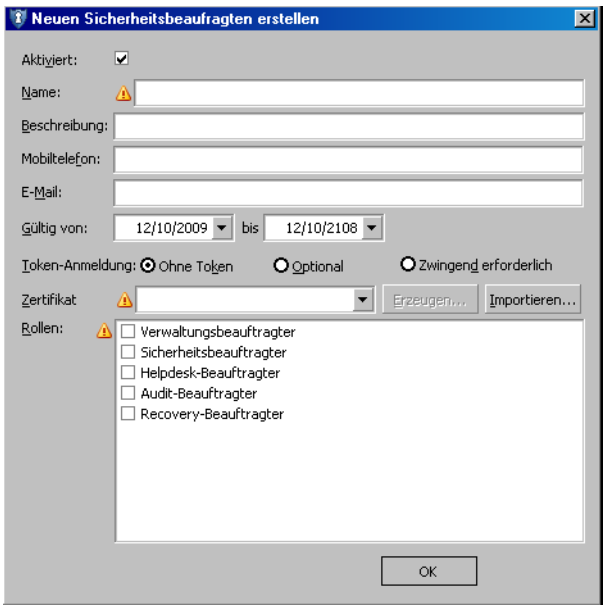
Der neu angelegte Haupt-Sicherheitsbeauftragte wird im Navigationsfenster unter dem Knoten **Haupt-Sicherheitsbeauftragte** angezeigt. Die jeweiligen Eigenschaften lassen sich durch Auswahl des gewünschten Sicherheitsbeauftragten im Navigationsfenster anzeigen. Der Haupt-Sicherheitsbeauftragte kann sich mit dem angezeigten Namen an das SafeGuard Management Center anmelden.

7.9 Sicherheitsbeauftragten anlegen

Voraussetzung: Um einen neuen Sicherheitsbeauftragten anzulegen, benötigen Sie das Recht Sicherheitsbeauftragte einzusehen und anzulegen.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Sicherheitsbeauftragten-Knoten, in dem Sie den neuen Sicherheitsbeauftragten anlegen möchten, und wählen Sie **Neu > Neuer Sicherheitsbeauftragter**.
3. Nehmen Sie die relevanten Einträge unter **Neuer Sicherheitsbeauftragter** vor:



Eingabefeld/Kontrollkästchen	Beschreibung
Aktiviert	Hier kann der Beauftragte bis auf Weiteres deaktiviert werden. Das bedeutet, dass er zwar im System existiert, sich aber noch nicht an das Management Center anmelden kann. Erst wenn er durch einen anderen Beauftragten aktiviert wird, kann er sich anmelden und seine administrativen Tätigkeiten ausführen.
Kurzname	Hier wird der Name des Beauftragten angegeben, wie er in den von SafeGuard Enterprise erzeugten Zertifikaten unter cn= eingetragen wird. Unter diesem Namen wird er auch im Navigationsfenster des Management Centers angezeigt. Dieser Name muss eindeutig sein. Maximalwert: 256 Zeichen
Beschreibung	Optional Maximalwert: 256 Zeichen
Mobiltelefon	Optional Maximalwert: 128 Zeichen
E-Mail	Optional Maximalwert: 256 Zeichen
Gültig von/bis	Hier wird angegeben, ab und bis wann (Datum) sich der Beauftragte am Management Center anmelden darf.
Token-Anmeldung	Die Anmeldung kann auf folgende Art erfolgen: **Ohne Token** Der Beauftragte darf sich nicht mit einem Token anmelden. Er muss sich über die Anmeldeinformationen (Benutzername/Kennwort) anmelden. **Optional** Die Anmeldung kann mit Token oder mit Anmeldeinformationen erfolgen. Der Sicherheitsbeauftragte kann wählen. **Zwingend erforderlich** Die Verwendung eines Token zur Anmeldung ist zwingend vorgeschrieben. Dazu muss sich der zum Zertifikat des Beauftragten gehörende private Schlüssel auf dem Token befinden.

Eingabefeld/Kontrollkästchen	Beschreibung
Zertifikat	Zur Anmeldung an das Management Center benötigt ein Beauftragter immer ein Zertifikat. Das Zertifikat kann entweder von SafeGuard Enterprise selbst erstellt werden oder es wird ein bereits existierendes verwendet. Ist eine Anmeldung mit Token zwingend notwendig, so muss das Zertifikat auf den Token des Sicherheitsbeauftragten aufgebracht werden. **Erzeugen:** Zertifikat und Schlüsseldatei werden neu erstellt und an einem auswählbaren Ort gespeichert. Dabei muss ein Kennwort für die .p12-Schlüsseldatei angegeben und bestätigt werden. Die .p12-Datei muss dem Sicherheitsbeauftragten bei der Anmeldung zur Verfügung stehen. Das erstellte Zertifikat wird dem Sicherheitsbeauftragten automatisch zugeteilt und unter **Zertifikat** angezeigt. Wenn SafeGuard Enterprise Kennwortregeln angewendet werden, sollten die Regeln im Active Directory deaktiviert werden. **Hinweis:** Maximale Länge des Speicherpfads und des Dateinamens: 260 Zeichen. Zum Anlegen eines Sicherheitsbeauftragten ist der öffentliche Teil des Zertifikats zwar ausreichend. Bei der Anmeldung am Management Center wird allerdings der private Teil des Zertifikats, die Schlüsseldatei, verlangt. Liegt diese nicht in der Datenbank vor, muss sie dem Sicherheitsbeauftragten zur Verfügung stehen und kann bei der Anmeldung dann ggf. im Zertifikatsspeicher abgelegt werden.
Zertifikat	**Importieren:** Ein existierendes Zertifikat wird importiert und anschließend dem Beauftragten zugewiesen. Wird aus einer .p12 Schlüsseldatei importiert, muss das Kennwort des Zertifikats bekannt sein. Wird ein PKCS#12 Zertifikatscontainer ausgewählt, werden alle Zertifikate in die Liste der zuweisbaren Zertifikate geladen. Die Zuweisung des Zertifikats erfolgt nach dem Import, indem das Zertifikat im Dropdown-Listenfeld ausgewählt wird.

Eingabefeld/Kontrollkästchen	Beschreibung
Rollen des Beauftragten	**Rollen** Dem Beauftragten können vordefinierte oder benutzerdefinierte Rollen zugewiesen werden. Die mit jeder Rolle verbundenen Rechte werden nach dem Klicken auf die entsprechende unter **zugelassene Aktion** im Aktionsbereich angezeigt. Zum Aufrufen der Rechte können Sie auch mit der rechten Maustaste auf den Sicherheitsbeauftragten klicken und **Eigenschaften, Aktionen** wählen. Einem Benutzer können mehrere Rollen zugewiesen werden. Vordefinierte Rollen werden fett dargestellt. Das Ausführen einer zusätzlichen Authentisierung ist ausdrücklich an den Besitz einer bestimmten Rolle gebunden.

4. Klicken Sie zur Bestätigung Ihrer Einstellungen auf **OK**.

Der neu angelegte Sicherheitsbeauftragte wird im Navigationsfenster unter dem jeweiligen **Sicherheitsbeauftragten**-Knoten angezeigt. Die jeweiligen Eigenschaften lassen sich durch Auswahl des gewünschten Sicherheitsbeauftragten im Navigationsfenster anzeigen.
Der Sicherheitsbeauftragte kann sich mit dem angezeigten Namen an das SafeGuard Management Center anmelden. Im nächsten Schritt müssen Sie nun dem Sicherheitsbeauftragten Verzeichnisobjekte/Domänen zuweisen, damit dieser die erforderlichen Aufgaben ausführen kann.

7.10 Einem Sicherheitsbeauftragten Verzeichnisobjekte zuweisen

Für die Ausführung ihrer Aufgaben benötigten Sicherheitsbeauftragte Zugriffsrechte für Verzeichnisobjekte. Unter dem Stammverzeichnis lässt sich der Zugriff auf Domänen- und Arbeitsgruppenknoten sowie auf den Knoten „Autoregistered“ gewähren.

Voraussetzung: Um einem Sicherheitsbeauftragten Verzeichnisobjekte zuzuweisen, benötigten Sie die Benutzer und Computer Rechte „Zugriffsrechte von Sicherheitsbeauftragten anzeigen“ und „Zugriffsrechte für Verzeichnis gewähren/verweigern“.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im Navigationsfenster auf der linken Seite die gewünschten Verzeichnisobjekte aus.

3. Klicken Sie im Aktionsbereich auf der rechten Seite auf die Registerkarte **Zugriff**.
4. Um die Rechte für die ausgewählten Objekte zuzuweisen, ziehen Sie den gewünschten Sicherheitsbeauftragten von der äußersten rechten Seite per Drag&Drop in die **Zugriff**-Tabelle. Um die Zuweisung rückgängig zu machen, ziehen Sie den Sicherheitsbeauftragten wieder zurück in die **Sicherheitsbeauftragte**-Tabelle.
5. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die ausgewählten Objekte stehen dem ausgewählten Sicherheitsbeauftragten zur Verfügung.

7.11 Benutzer und Sicherheitsbeauftragte befördern

Sie haben folgende Möglichkeiten:

- Sie können einen Benutzer im Bereich **Benutzer & Computer** zum Sicherheitsbeauftragten machen.
- Sie können einen Sicherheitsbeauftragten im Bereich **Sicherheitsbeauftragte** zu einem Haupt-Sicherheitsbeauftragten machen.

7.11.1 Voraussetzungen für die Ernennung eines Benutzers zum Sicherheitsbeauftragten

Ein Sicherheitsbeauftragter mit den erforderlichen Rechten kann Benutzer zu Sicherheitsbeauftragten machen und ihnen Rollen zuweisen.

Auf diese Weise ernannte Sicherheitsbeauftragte können sich mit Ihren Windows-Anmeldeinformationen oder ihrer Token/Smartcard-PIN an das SafeGuard Management Center anmelden. Sie können genauso wie andere Sicherheitsbeauftragte agieren und verwaltet werden.

Folgende Voraussetzungen müssen erfüllt sein:

- Benutzer, die zu Sicherheitsbeauftragten ernannt werden sollen, müssen aus einem Active Directory importiert und im SafeGuard Management Center unter **Benutzer & Computer** sichtbar sein.
- Damit sich ein zum Sicherheitsbeauftragten ernannter Benutzer an das SafeGuard Management Center anmelden kann, muss ein Benutzerzertifikat ausgestellt oder importiert und zugewiesen sein. Für die Anmeldung mit den Windows-Anmeldeinformationen muss die .p12-Datei mit dem privaten Schlüssel in der SafeGuard Enterprise Datenbank vorhanden sein. Für die Anmeldung mit Token bzw. Smartcard-PIN muss sich die .p12-Datei mit dem privaten Schlüssel auf dem Token bzw. der Smartcard befinden.

7.11.2 Einen Benutzer zum Sicherheitsbeauftragten machen

Voraussetzung: Nur Haupt-Sicherheitsbeauftragte dürfen einen Benutzer zum Sicherheitsbeauftragten machen.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie den Benutzer aus, den Sie zum Sicherheitsbeauftragten machen möchten, und klicken Sie auf die Registerkarte **Zertifikat** im Aktionsbereich auf der rechten Seite.

- Wenn dem Benutzer ein Zertifikat zugeordnet ist, wird es im Aktionsbereich angezeigt.
- Wenn dem Benutzer noch kein Zertifikat zugeordnet ist, klicken Sie zum Zuweisen auf das Symbol **Zertifikat importieren** in der Symbolleiste. Wählen Sie den notwendigen Zertifikatsspeicher (*.cer) sowie die private Schlüsseldatei (*.p12) und bestätigen Sie die Auswahl mit **OK**.

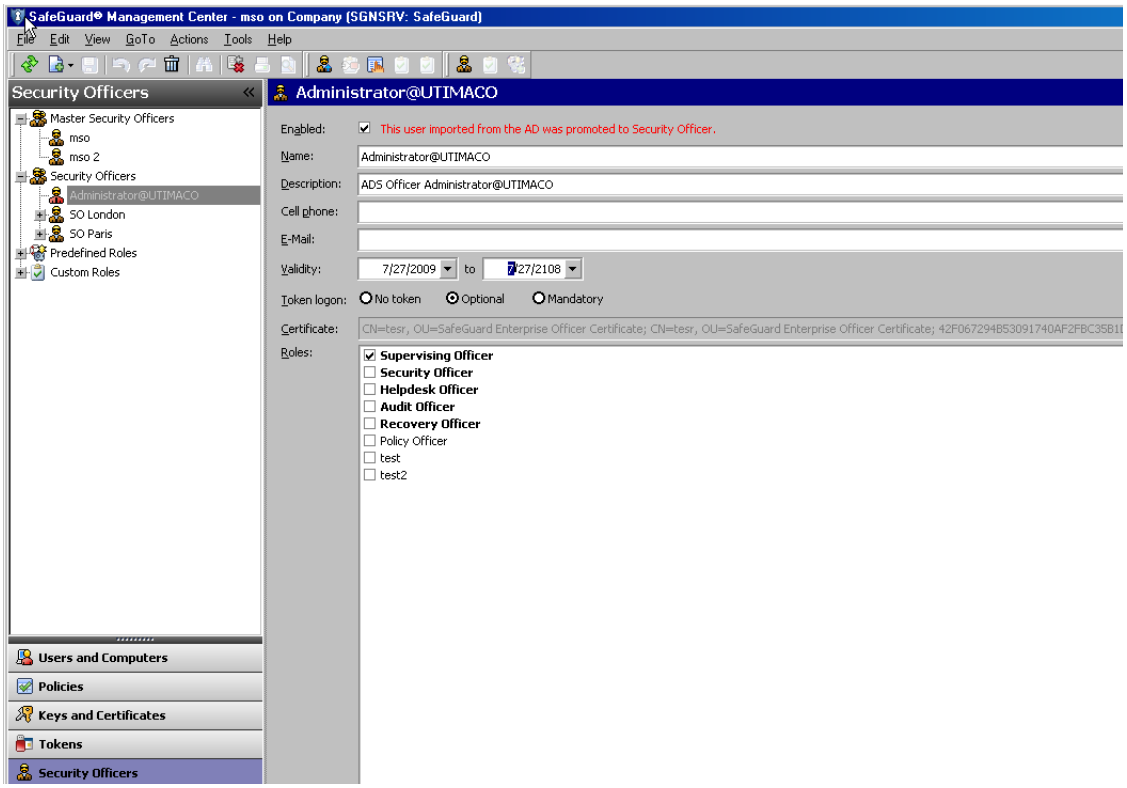
3. Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie zum Sicherheitsbeauftragten machen möchten. Wählen Sie **Diesen Benutzer zum Sicherheitsbeauftragten machen**.
4. Aktivieren Sie unter **Rollenauswahl** die gewünschte(n) Rolle(n) durch Anklicken und bestätigen Sie mit **OK**.

   Vordefinierte Rollen werden fett dargestellt. Sind einem untergeordnetem Sicherheitsbeauftragten mehr Rollen zugeordnet als dem angemeldeten Sicherheitsbeauftragten, so werden diese Rollen kursiv dargestellt.
5. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Der Benutzer ist nun Sicherheitsbeauftragter und wird im Bereich **Sicherheitsbeauftragte** mit seinem Benutzernamen angezeigt. Seine Eigenschaften lassen sich durch Auswahl des Sicherheitsbeauftragten im Navigationsfenster anzeigen. Ist der private Schlüssel des Benutzers in der Datenbank gespeichert, so ist **Kein Token** aktiviert. Wenn sich der private Schlüssel auf dem Token oder der Smartcard befindet, ist **Optional** aktiviert.

Nach Wunsch können Sie den Sicherheitsbeauftragten per Drag&Drop auf der gewünschten Position in der Baumstruktur des Bereichs **Sicherheitsbeauftragte** platzieren.

Der Sicherheitsbeauftragte kann sich nun mit dem angezeigten Namen an das SafeGuard Management Center anmelden.



7.11.3 Einen Sicherheitsbeauftragten zum Haupt-Sicherheitsbeauftragten machen

Voraussetzung: Um einen Sicherheitsbeauftragten zum Haupt-Sicherheitsbeauftragten zu machen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu modifizieren.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Sicherheitsbeauftragten, den Sie zum Haupt-Sicherheitsbeauftragten machen möchten. Wählen Sie **Zum Haupt-Sicherheitsbeauftragten ernennen**.
3. Weist der ausgewählte Sicherheitsbeauftragte untergeordnete Sicherheitsbeauftragte auf, so werden Sie dazu aufgefordert, einen neuen übergeordneten Knoten für diese untergeordneten Sicherheitsbeauftragten auszuwählen.

Der Sicherheitsbeauftragte wird zum Haupt-Sicherheitsbeauftragten gemacht und unter dem Knoten **Haupt-Sicherheitsbeauftragte** angezeigt. Als Haupt-Sicherheitsbeauftragter erhält der ernannte Sicherheitsbeauftragte alle Rechte auf alle Objekte und verliert somit alle zugewiesenen Rollen sowie einzeln gewährte Domänen-Zugriffsberechtigungen im Bereich **Benutzer und Computer**.

7.12 Ernennung zum Haupt-Sicherheitsbeauftragten rückgängig machen

Voraussetzung: Nur Haupt-Sicherheitsbeauftragte können die Ernennung von Sicherheitsbeauftragten zu Haupt-Sicherheitsbeauftragten rückgängig machen,

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Haupt-Sicherheitsbeauftragten, dessen Ernennung Sie rückgängig machen möchten. Wählen Sie **Zum Sicherheitsbeauftragten zurückstufen**.
3. Sie werden dazu aufgefordert, einen übergeordneten Knoten für den Sicherheitsbeauftragten zu wählen und mindestens eine Rolle zuzuweisen.

Die Ernennung des Sicherheitsbeauftragten zum Haupt-Sicherheitsbeauftragten wird rückgängig gemacht und der Sicherheitsbeauftragte wird unter dem ausgewählten **Sicherheitsbeauftragten**-Knoten angezeigt. Der Sicherheitsbeauftragte verliert alle Rechte für alle Objekte und erhält nur die Rechte, die den zugewiesenen Rollen zugeordnet sind. Ein Sicherheitsbeauftragter, dessen Ernennung zum Haupt-Sicherheitsbeauftragten rückgängig gemacht wurde, hat zunächst keine Domänen-Zugriffsrechte. Domänen-Zugriffsrechte müssen einzeln im Bereich **Benutzer & Computer** in der Registerkarte **Zugriff** gewährt werden.

7.13 Zertifikat eines Sicherheitsbeauftragten ändern

Voraussetzung: Um das Zertifikat eines Sicherheitsbeauftragten oder Haupt-Sicherheitsbeauftragten zu ändern, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu modifizieren.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Sicherheitsbeauftragten, dessen Zertifikat Sie ändern möchten. Das aktuelle Zertifikat wird im Aktionsbereich auf der rechten Seite unter **Zertifikate** angezeigt.
3. Klicken Sie im Aktionsbereich auf die Dropdownliste **Zertifikate** und wählen Sie ein anderes Zertifikat aus.
4. Klicken Sie auf das **Speichern**-Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

7.14 Sicherheitsbeauftragte in der Baumstruktur anordnen

Sicherheitsbeauftragte lassen sich im Navigationsbereich des SafeGuard Management Center gemäß der Organisationsstruktur Ihres Unternehmens hierarchisch anordnen.

Die Baumstruktur lässt sich für alle Sicherheitsbeauftragten, außer für Haupt-Sicherheitsbeauftragte, ordnen. Haupt-Sicherheitsbeauftragte werden in einer nicht-hierarchischen Liste unter dem Haupt-Sicherheitsbeauftragten-Knoten angezeigt.
Der Sicherheitsbeauftragten-Knoten enthält eine Baumstruktur, in der jeder Knoten einen Sicherheitsbeauftragten repräsentiert. Diese hierarchische Anordnung gibt jedoch keine Hierarchie in Bezug auf Rechte und Rollen wieder.

Voraussetzung: Um einen Sicherheitsbeauftragten in der Baumstruktur zu verschieben, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu modifizieren.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Ziehen Sie im den gewünschten Sicherheitsbeauftragten im Navigationsfenster per Drag&Drop zum gewünschten Knoten.

Alle dem Sicherheitsbeauftragten untergeordneten Sicherheitsbeauftragte werden ebenfalls verschoben.

7.15 Schneller Wechsel zwischen Sicherheitsbeauftragten

Sie können das SafeGuard Management Center schnell und einfach neu starten, wenn Sie sich mit einem anderen Sicherheitsbeauftragten anmelden möchten.

Gehen Sie wie folgt vor:

1. Wählen Sie im SafeGuard Management Center **Datei > Sicherheitsbeauftragten wechseln**. Das SafeGuard Management Center wird neu gestartet und es wird ein Anmeldedialog angezeigt.
2. Wählen Sie den Sicherheitsbeauftragten, mit dem Sie sich an das SafeGuard Management Center anmelden möchten, und geben Sie das zugehörige Kennwort ein. Wenn Sie im Multi Tenancy Modus arbeiten, werden Sie wieder an dieselbe Datenbankkonfiguration angemeldet.

Das SafeGuard Management Center wird neu gestartet und zeigt die dem angemeldeten Sicherheitsbeauftragten zugeordnete Ansicht.

7.16 Sicherheitsbeauftragten löschen

Voraussetzung: Um einen Sicherheitsbeauftragten zu löschen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu löschen.

Gehen Sie wie folgt vor:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Sicherheitsbeauftragten oder den Haupt-Sicherheitsbeauftragten, den Sie löschen möchten. Wählen Sie **Löschen**. Beachten Sie, dass Sie den Sicherheitsbeauftragten, mit dem Sie angemeldet sind, nicht löschen können.
3. Weist der ausgewählte Sicherheitsbeauftragte untergeordnete Sicherheitsbeauftragte auf, so werden Sie dazu aufgefordert, einen neuen übergeordneten Knoten für diese untergeordneten Sicherheitsbeauftragten auszuwählen.

Der Sicherheitsbeauftragte wird aus der Datenbank gelöscht.

Hinweis: Mindestens ein Haupt-Sicherheitsbeauftragter, der explizit als Beauftragter angelegt wurde und nicht nur zum Haupt-Sicherheitsbeauftragten ernannt wurde, muss immer in der Datenbank verbleiben. Wird ein Benutzer, der zum Sicherheitsbeauftragten ernannt wurde, aus der Datenbank gelöscht, so wird auch sein Benutzerkonto aus der Datenbank gelöscht.

Hinweis: Wenn der zu löschende Sicherheitsbeauftragte eine Rolle hat, die zusätzliche Autorisierung umfasst und dem Sicherheitsbeauftragten als einziger diese Rolle zugewiesen ist, wird der Sicherheitsbeauftragte trotzdem gelöscht. Es wird angenommen, dass der Haupt-Sicherheitsbeauftragte die zusätzliche Autorisierung übernimmt.

8 Datenverschlüsselung

Ein Kernstück von SafeGuard Enterprise ist die Verschlüsselung von Daten auf unterschiedlichen Datenträgern. Die Verschlüsselung kann volume- oder dateibasierend durchgeführt werden, mit unterschiedlichen Schlüsseln und Algorithmen.

Dateien werden transparent verschlüsselt. Wenn Benutzer Dateien öffnen, bearbeiten und speichern, werden Sie nicht zur Ver- oder Entschlüsselung aufgefordert.

Als Sicherheitsbeauftragter legen Sie die Einstellungen für die Verschlüsselung in einer Sicherheitsrichtlinie vom Typ **Geräteschutz** fest.

8.1 Volume-basierende Verschlüsselung

Mit der volume-basierenden Verschlüsselung werden alle Daten auf einem Volume (einschließlich Boot-Dateien, Pagefiles, Hibernation Files, temporäre Dateien, Verzeichnisinformationen usw.) verschlüsselt. Benutzer müssen sich in ihrer Arbeitsweise nicht anpassen oder auf Sicherheit achten.

Hinweis: Wenn für ein Volume oder einen Volume-Typ eine Verschlüsselungsrichtlinie existiert und die Verschlüsselung des Volumes schlägt fehl, darf der Benutzer nicht auf das Volume zugreifen.

Um volume-basierende Verschlüsselung auf Endpoint-Computer anzuwenden, erstellen Sie eine Richtlinie vom Typ **Geräteschutz** und wählen Sie bei **Verschlüsselungsmodus für Medien** die Einstellung **Volume-basierend**.

8.1.1 Schnelle Initialverschlüsselung

SafeGuard Enterprise bietet die schnelle Initialverschlüsselung als Spezialmodus für die volume-basierende Verschlüsselung. Dieser Modus reduziert den Zeitraum, der für die initiale Verschlüsselung (oder die endgültige Entschlüsselung) von Volumes auf Endpoint-Computern benötigt wird. Dies wird dadurch erreicht, dass nur auf den Festplattenspeicherplatz zugegriffen wird, der tatsächlich in Gebrauch ist.

Für die schnelle Initialverschlüsselung gelten folgende Voraussetzungen:

- Die schnelle Initialverschlüsselung funktioniert nur auf NTFS-formatierten Volumes.
- Bei NTFS-formatierten Volumes mit einer Cluster-Größe von 64 KB kann die schnelle Initialverschlüsselung nicht angewendet werden.

Hinweis: Dieser Modus kann zu einem unsichereren Zustand führen, wenn eine Platte vor der Verwendung mit SafeGuard Enterprise bereits in Gebrauch war. Nicht verwendete Sektoren können noch Daten enthalten. Daher ist die schnelle Initialverschlüsselung standardmäßig deaktiviert.

Um die schnelle Initialverschlüsselung zu aktivieren, wählen Sie die Einstellung **Schnelle Initialverschlüsselung** in einer Richtlinie vom Typ **Geräteschutz**.

Hinweis: Für die Entschlüsselung eines Volumes wird unabhängig von der gewählten Richtlinieneinstellung immer die schnelle Initialverschlüsselung verwendet. Für die Entschlüsselung gelten ebenfalls die angegebenen Einschränkungen.

8.1.2 Volume-basierende Verschlüsselung und die Windows 7 Systempartition

Für Windows 7 Professional, Enterprise und Ultimate wird auf den Endpoint-Computern eine Systempartition angelegt, der kein Laufwerksbuchstabe zugeordnet ist. Diese System-Partition kann nicht von SafeGuard Enterprise verschlüsselt werden.

8.1.3 Volume-basierende Verschlüsselung und Unidentified File System Objects

Unidentified File System Objects sind Volumes, die von SafeGuard Enterprise nicht eindeutig als verschlüsselt oder unverschlüsselt identifiziert werden können. Existiert für ein Unidentified File System Object eine Verschlüsselungsrichtlinie, so wird der Zugriff auf das Volume verweigert. Existiert keine Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen.

Hinweis: Existiert für ein Unidentified File System Object eine Verschlüsselungsrichtlinie, bei der die Richtlinieneinstellung **Schlüssel für die Verschlüsselung** auf eine Option eingestellt ist, die die Schlüsselauswahl ermöglicht (z. B. **Beliebiger Schlüssel im Schlüsselring des Benutzer**), so entsteht zwischen der Anzeige des Schlüsselauswahldialogs und der Verweigerung des Zugriffs auf das Volume eine zeitliche Lücke. Während dieser Zeit kann auf das Volume zugegriffen werden. So lange der Schlüsselauswahldialog nicht vom Benutzer bestätigt wird, besteht Zugriff auf das Volume. Um dies zu vermeiden, geben Sie einen vorausgewählten Schlüssel für die Verschlüsselung an. Diese zeitliche Lücke entsteht auch dann für mit dem Endpoint-Computer verbundene Unidentified File System Objects, wenn der Benutzer zu dem Zeitpunkt, an dem die Verschlüsselungsrichtlinie wirksam wird, bereits Dateien auf dem Volume geöffnet hat. In diesem Fall, kann nicht gewährleistet werden, dass der Zugriff auf das Volume verweigert wird, da dies zu Datenverlust führen könnte.

8.1.4 Verschlüsselung von Volumes mit aktivierter Autorun-Funktionalität

Wenn Sie auf Volumes, für die die Autorun-Funktionalität aktiviert ist, eine Verschlüsselungsrichtlinie anwenden, so können folgende Probleme auftreten:

- Das Volume wird nicht verschlüsselt.
- Wenn es sich bei dem Volume um ein Unidentified File System Object (siehe *Volume-basierende Verschlüsselung und Unidentified File System Objects* auf Seite 64) handelt, so wird der Zugriff nicht verweigert.

8.1.5 Zugriff auf mit BitLocker To Go verschlüsselte Volumes

Wird SafeGuard Enterprise mit aktivierter BitLocker To Go Unterstützung verwendet und existiert eine SafeGuard Enterprise Verschlüsselungsrichtlinie für ein mit BitLocker To Go verschlüsseltes Volume, so wird der Zugriff auf das Volume verweigert. Existiert keine SafeGuard Enterprise Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen.

Hinweis: Wenn die Autorun-Einstellungen für ein mit BitLocker To Go verschlüsseltes Volume auf die Standardwerte eingestellt sind, kann es vorkommen, dass der Zugriff trotz vorhandener SafeGuard Enterprise Verschlüsselungsrichtlinie nicht verweigert wird. Diese Situation tritt nur unter Windows Vista auf.

8.2 Dateibasierende Verschlüsselung

Die dateibasierende Verschlüsselung stellt sicher, dass alle Daten verschlüsselt sind (außer Boot Medium und Verzeichnisinformationen). Mit dateibasierender Verschlüsselung lassen sich auch optische Medien wie CD/DVD verschlüsseln. Außerdem können Daten mit Fremdrechnern, auf denen SafeGuard Enterprise nicht installiert ist, ausgetauscht werden (soweit von der Richtlinie erlaubt).

Hinweis: Mit “Dateibasierender Verschlüsselung” verschlüsselte Daten können nicht komprimiert werden. Umgekehrt können auch komprimierte Dateien nicht dateibasierend verschlüsselt werden.

Hinweis: Boot-Volumes werden niemals dateibasierend verschlüsselt. Sie sind automatisch von einer dateibasierenden Verschlüsselung ausgenommen, auch wenn eine entsprechende Regel definiert ist.

Um dateibasierende Verschlüsselung auf Endpoint-Computer anzuwenden, erstellen Sie eine Richtlinie vom Typ **Geräteschutz** und wählen Sie bei **Verschlüsselungsmodus für Medien** die Einstellung **Dateibasierend**.

8.2.1 Anwendungen von der Verschlüsselung ausnehmen

Sie können für Anwendungen festlegen, dass sie vom SafeGuard Enterprise Filter-Treiber ignoriert werden sollen. Damit sind sie von der transparenten Ver-/Entschlüsselung ausgenommen.

Ein Beispiel hierfür ist ein Backup- Programm. Damit die Daten beim Erstellen eines Backups nicht entschlüsselt werden, kann diese Anwendung von der Verschlüsselung/Entschlüsselung ausgenommen werden. Die Daten werden verschlüsselt gesichert.

Als typischer Anwendungsfall können Backup-Programme zum Beispiel als unberücksichtigt definiert werden, damit sie immer die verschlüsselten Daten lesen und sichern.

Anwendungen, die bei gleichzeitiger Verwendung mit SafeGuard Enterprise Funktionsstörungen auslösen können, aber keine Verschlüsselung erfordern, können generell von der Verschlüsselung ausgenommen werden.

Sie können Anwendungen von der Verschlüsselung/Entschlüsselung in einer Richtlinie vom Typ **Geräteschutz** mit dem Ziel **Lokale Datenträger** ausnehmen. Zur Angabe von **Unberücksichtigten Anwendungen** wird der vollständige Name der ausführbaren Datei (optional inklusive Pfadinformation) verwendet.

9 SafeGuard Enterprise Schlüsselmanagement

SafeGuard Enterprise erzeugt in der Standardeinstellung beim Import der Verzeichnisstruktur automatisch Schlüssel für:

- Domänen
- Container/OUs
- Gruppen

und weist diese den entsprechenden Objekten zu. Computer- und Benutzerschlüssel werden bei Bedarf erzeugt.

Schlüssel können nicht gelöscht werden! Sie sind immer in der SafeGuard Enterprise Datenbank enthalten.

Beim ersten Starten eines Endpoint-Computers erzeugt SafeGuard Enterprise einen Computerschlüssel für diesen Computer (definierter Computerschlüssel).

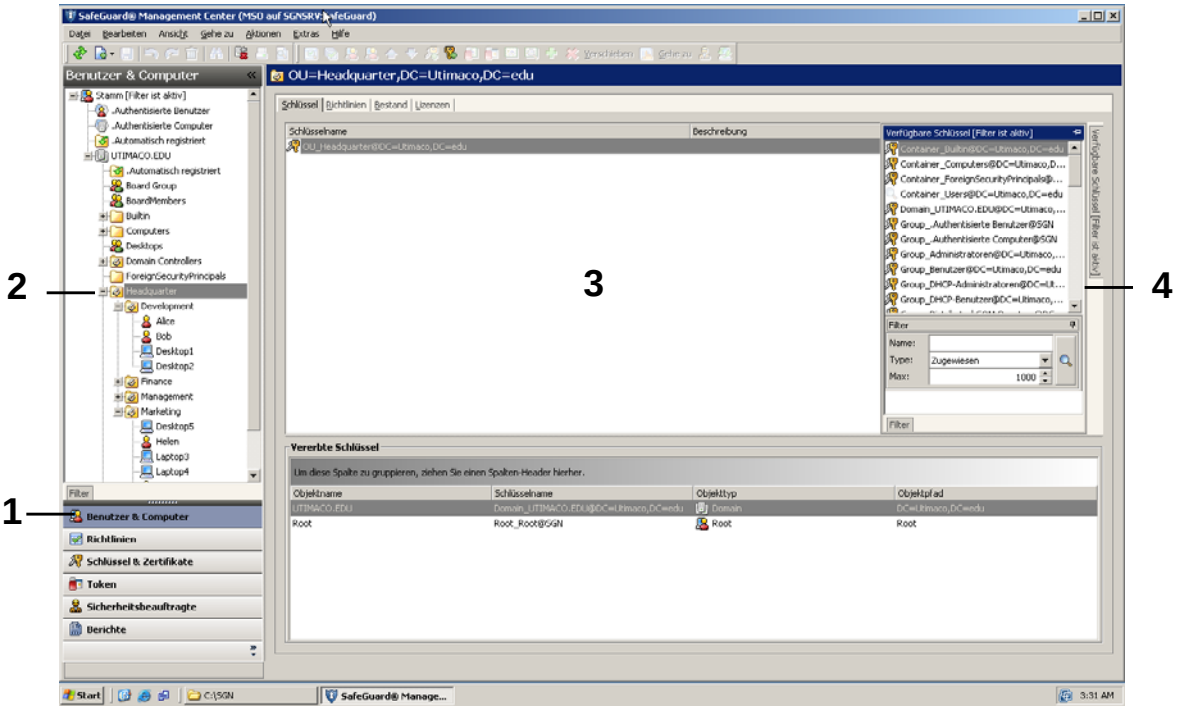
Bei der Anmeldung erhält jeder Benutzer alle Schlüssel aus seinem Schlüsselbund.
Dieser Schlüsselbund besteht aus:

- einem persönlichen Schlüssel
- aus den Schlüsseln der Gruppen, in denen der Benutzer Mitglied ist.
- aus den Schlüsseln der den Gruppen, in denen er Mitglied ist, übergeordneten Container/ OUs.

Durch die Schlüssel in seinem Schlüsselbund ist festgelegt, auf welche Daten der Benutzer zugreifen kann. Es ist dem Benutzer nur möglich, auf Daten zuzugreifen, für die er den passenden Schlüssel besitzt.

Alle vorhandenen Schlüssel werden angezeigt, wenn Sie im Navigationsbereich des SafeGuard Management Centers auf **Benutzer & Computer** klicken und die Registerkarte **Schlüssel** wählen.

Alle überhaupt vohandenen Schlüssel können angezeigt werden, wenn Sie im Navigationsbereich des SafeGuard Management Centers auf **Schlüssel & Zertifikate** klicken und **Zugewiesene Schlüssel** bzw. **Inaktive Schlüssel** auswählen. Für alle Schlüssel können Sie sich dort Listen generieren lassen.

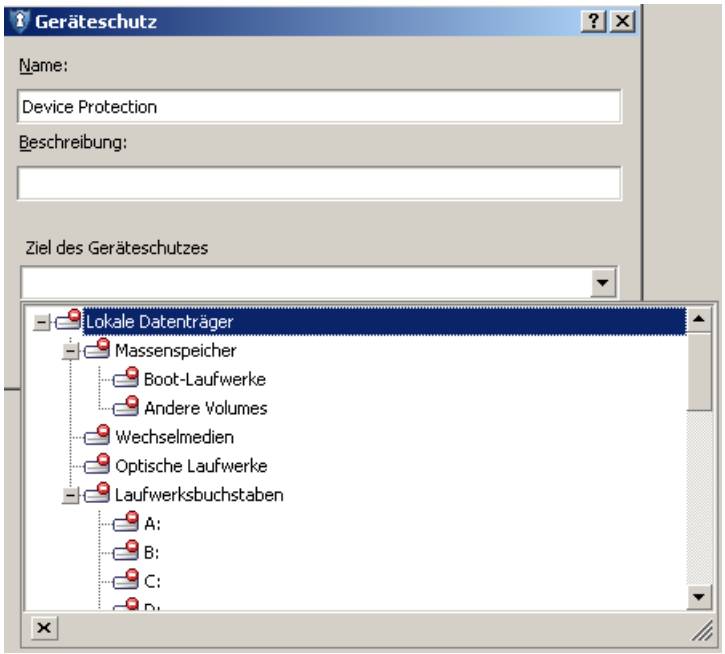


1. Diese Ansicht wird durch Klicken auf **Benutzer & Computer** geöffnet.
2. Die Schlüssel eines hier markierten Objekts werden im Aktionsbereich und in den dazugehörigen Ansichten angezeigt
3. Aktionsbereich: Anzeige abhängig von der Auswahl im Navigationsbereich. Es werden alle dem Objekt zugewiesenen Schlüssel angezeigt.
4. Hier werden alle verfügbaren Schlüssel angezeigt. Dem ausgewählten Objekt bereits zugewiesene Schlüssel sind ausgegraut. Über **Filter** kann zwischen bereits einem Objekt zugewiesenen (aktiven) und noch keinem Objekt zugewiesenen (inaktiven) Schlüsseln umgeschaltet werden.

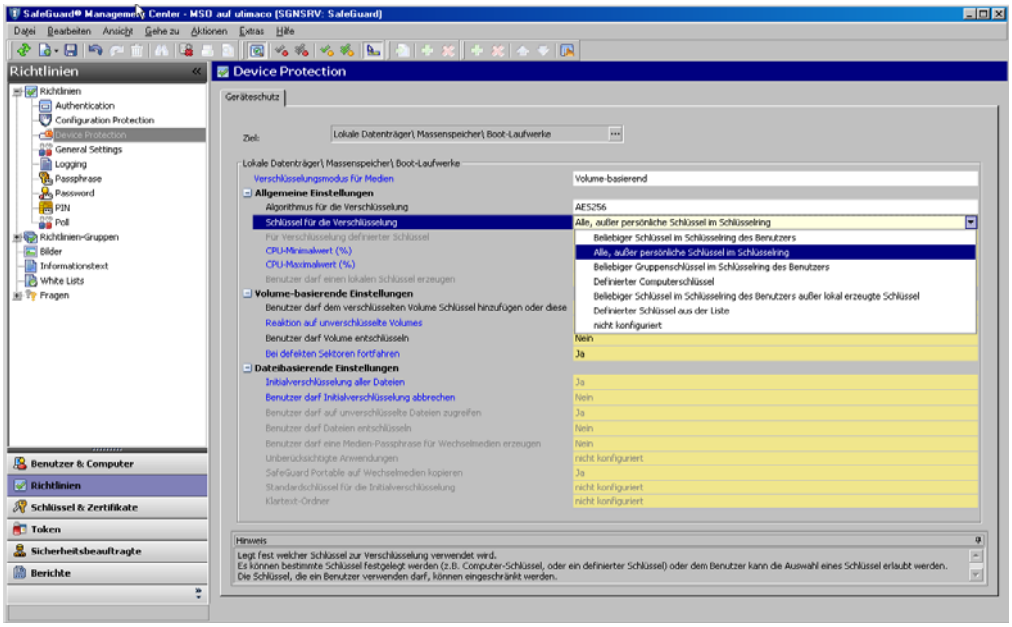
Nach dem Import verfügt jeder Benutzer über eine Anzahl von Schlüsseln, die zur Datenverschlüsselung verwendet werden können.

9.1 Schlüssel für die Datenverschlüsselung

Benutzern können bestimmte Schlüssel zur Verschlüsselung von Volumes zugewiesen werden, indem Richtlinien vom Typ **Geräteschutz** angelegt werden. Folgende Volumes stehen zur Verfügung:



Wenn Sie die Einstellungen für die verschiedenen Medien vornehmen, finden Sie bei jedem Medium die Option: **Schlüssel für die Verschlüsselung**.



Hier können Sie festlegen, welche Schlüssel der Benutzer bei der Verschlüsselung verwenden darf bzw. muss:

- **Beliebiger Schlüssel im Schlüsselring des Benutzers**
  Der Benutzer kann nach der Anmeldung an Windows auswählen, welchen Schlüssel er für die Verschlüsselung des Laufwerks verwenden möchte.
  Es wird ein Dialog angezeigt, in dem der Benutzer den gewünschten Schlüssel auswählen kann.

- **Alle, außer persönliche Schlüssel im Schlüsselring**
  Ein Benutzer darf seinen persönlichen Schlüssel nicht verwenden, um Daten zu verschlüsseln.

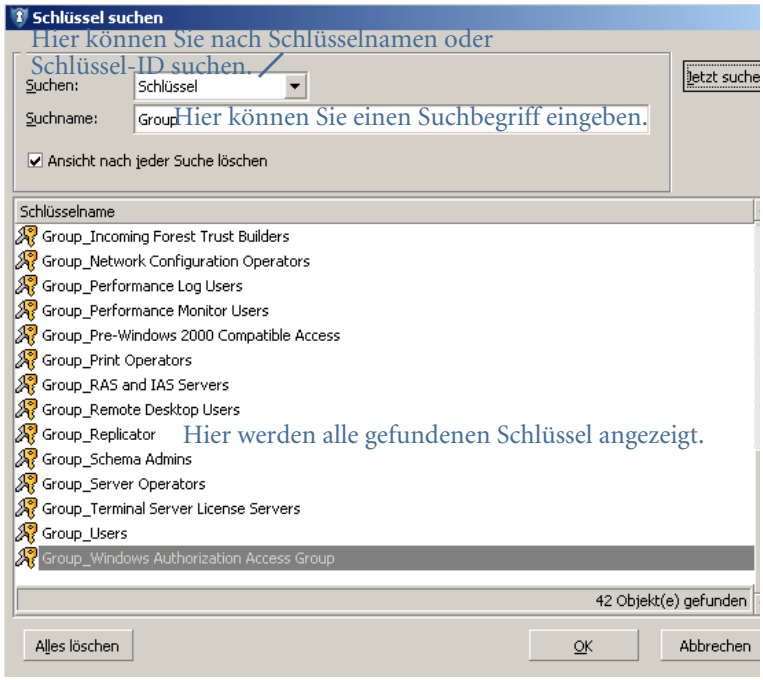
- **Beliebiger Gruppenschlüssel im Schlüsselring des Benutzers**
  Der Benutzer darf nur aus den in seinem Schlüsselbund vorhandenen Gruppenschlüsseln auswählen.

- **Definierter Computerschlüssel**
  Ist der eindeutige Schlüssel, der beim ersten Hochfahren des Computers exklusiv für diesen Computer in SafeGuard Enterprise erzeugt wird. Der Benutzer hat keine Auswahlmöglichkeit.

  Ein definierter Computerschlüssel wird nur für die Boot- und Systempartition eingesetzt und für Laufwerke, auf denen sich Dokumente und Einstellungen befinden.

- **Definierter Schlüssel aus der Liste**
  Diese Option erlaubt es Ihnen, einen bestimmten Schlüssel zu definieren, der vom Benutzer zur Verschlüsselung verwendet werden muss. Wenn Sie dem Benutzer einen Schlüssel auf diese Weise vorgeben wollen, müssen Sie unter **Für Verschlüsselung definierter Schlüssel** (wird erst angezeigt, wenn die Option **Definierter Schlüssel aus der Liste** ausgewählt wurde) einen Schlüssel festlegen.

  Wenn Sie auf die **[...]** Schaltfläche neben der Option **Für Verschlüsselung definierter Schlüssel** klicken, wird ein Dialog angezeigt, in dem Sie einen Schlüssel angeben können. Stellen Sie sicher, dass der Benutzer auch im Besitz des entsprechenden Schlüssels ist, wenn Sie so die Verwendung eines bestimmten Schlüssels festlegen.



Markieren Sie den gewünschten Schlüssel und klicken Sie auf **OK**.

Der ausgewählte Schlüssel wird auf dem Benutzer-Computer zur Verschlüsselung verwendet.

9.2 Zertifikate

- SafeGuard Enterprise kann mit signierten SHA1, MD2 und MD5 Zertifikaten verifiziert werden.
- Wenn Certification Authority (CA) Zertifikate in der Datenbank gelöscht werden und Sie diese nicht mehr verwenden möchten, sollten Sie diese Zertifikate manuell von allen Administrator PCs im lokalen Speicher entfernen.
- SafeGuard Enterprise kann in diesem Fall nur dann mit abgelaufenen Zertifikaten kommunizieren, wenn sich alte und neue Schlüssel auf derselben Karte befinden.
- Die Kombination aus CA Zertifikaten und CRL (Certificate Revocation List) Zertifikaten auf einer Smartcard muss übereinstimmen. Andernfalls können sich die Benutzer nicht an den entsprechenden Computern anmelden. Bitte überprüfen Sie, ob die Kombination korrekt ist. SafeGuard Enterprise führt diese Überprüfung nicht durch.
- Die Anmeldezertifikate für Sicherheitsbeauftragte müssen sich in “MY” befinden.
- CA Zertifikate können nicht von einem Token entnommen und in der Datenbank oder im Zertifikatsspeicher gespeichert werden. Wenn Sie CA Zertifikate verwenden möchten (oder müssen), müssen diese in Dateiform zur Verfügung stehen, nicht nur auf einem Token. Dies gilt auch für CRLs.
- Beachten Sie, dass beim Importieren eines Benutzerzertifikats sowohl der öffentliche als auch der private Bereich des Zertifikats importiert werden. Wird nur der öffentliche Bereich importiert, so wird nur die Anmeldung mit Token unterstützt.

9.3 Virtuelle Clients

Virtuelle Clients sind spezifische verschlüsselte Schlüsseldateien, die im Rahmen eines Challenge/Response-Verfahrens für Recovery-Zwecke verwendet werden können, wenn die benötigten Benutzerinformationen nicht zur Verfügung stehen und ein Challenge/Response-Verfahren normalerweise nicht möglich wäre (z. B. bei beschädigter POA).

Um in dieser komplexen Notfallsituation ein Challenge/Response-Verfahren zu ermöglichen, lassen sich spezifische Dateien, die als virtuelle Clients bezeichnet werden, erstellen. Diese Dateien müssen vor dem Challenge/Response-Verfahren an den Benutzer verteilt werden. Daraufhin lässt sich mit Hilfe der virtuellen Clients ein Challenge/Response-Verfahren über ein Schlüssel-Recovery Tool auf dem Endpoint-Computer starten. Der Benutzer muss dann nur den Helpdesk-Beauftragten über den/die benötigten Schlüssel informieren und den Response-Code eingeben, um wieder Zugriff auf das verschlüsselte Volume zu erhalten.

Der Zugriff kann entweder mit Hilfe eines einzelnen Schlüssels oder mit Hilfe einer verschlüsselten Schlüsseldatei, die mehrere Schlüssel enthält, wiederhergestellt werden.

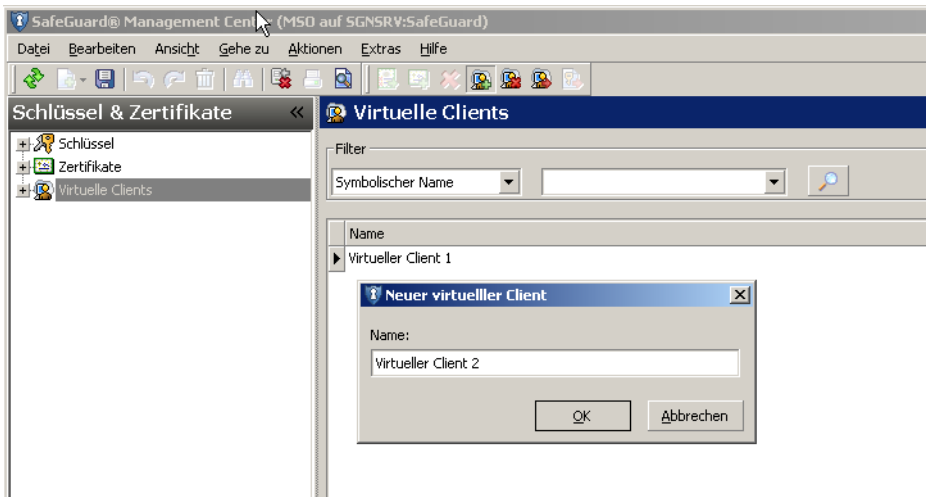
Im Bereich **Schlüssel & Zertifikate** des SafeGuard Management Centers haben Sie folgende Möglichkeiten:

- Virtuelle Clients anlegen und exportieren
- Verschlüsselte Schlüsseldateien mit mehreren Schlüsseln anlegen und exportieren
- Virtuelle Clients und exportierte Schlüsseldateien anzeigen lassen und filtern
- Virtuelle Clients löschen

9.3.1 Virtuelle Clients anlegen

Virtuelle Client-Dateien können von verschiedenen Computern und für mehrere Challenge/Response-Verfahren genutzt werden.

1. Öffnen Sie das SafeGuard Management Center und klicken Sie auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.



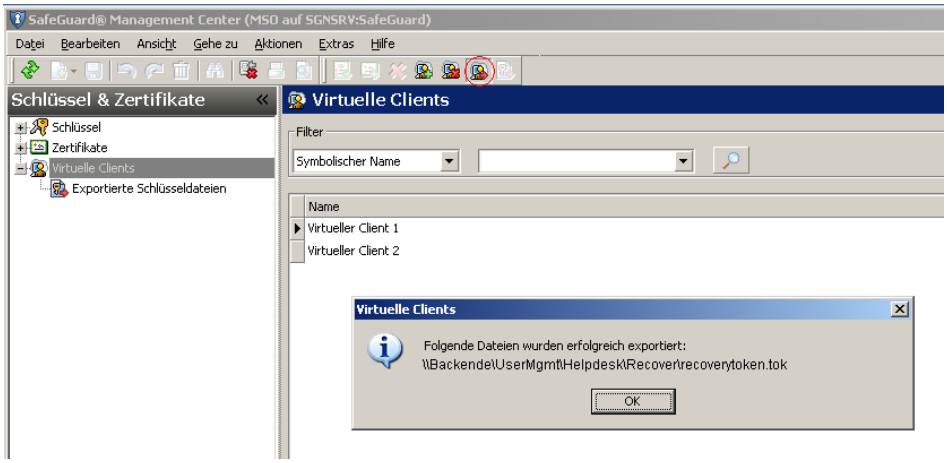
3. Klicken Sie in der Symbolleiste auf **Virtuellen Client hinzufügen**.
4. Geben Sie einen eindeutigen Namen für den virtuellen Client ein und klicken Sie auf **OK**. Die virtuellen Clients werden anhand der hier eingegebenen Namen in der Datenbank identifiziert.
5. Speichern Sie den virtuellen Client in der Datenbank, indem Sie in der Symbolleiste auf das Symbol **Speichern** klicken.

Der neue virtuelle Client wird im Aktionsbereich angezeigt.

9.3.2 Virtuelle Clients exportieren

Nach dem Anlegen des virtuellen Client muss dieser in eine Datei exportiert werden. Diese Datei hat immer die Bezeichnung `recoverytoken.tok` und muss an die Benutzer verteilt werden. Beim Starten eines Challenge/Response-Verfahrens über ein Recovery Tool, z. B. bei einer beschädigten POA, muss diese Datei dem Benutzer zur Verfügung stehen. Der Benutzer muss die Datei `recoverytoken.tok` im selben Verzeichnis, in dem sich auch das Recovery Tool befindet, ablegen, damit ein Challenge/Response-Verfahren unterstützt wird.

1. Öffnen Sie das SafeGuard Management Center und klicken Sie auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.



3. Suchen Sie im Aktionsbereich nach dem entsprechenden virtuellen Client, indem Sie auf das Lupensymbol klicken. Die verfügbaren virtuellen Clients werden angezeigt.
4. Wählen Sie den gewünschten Eintrag im Aktionsbereich aus und klicken Sie in der Symbolleiste auf **Virtuellen Client exportieren**.
5. Wählen Sie einen Speicherort für die Datei `recoverytoken.tok` und klicken Sie auf **OK**.
6. Eine Meldung, die Sie über das erfolgreiche Speichern sowie den Speicherort der Datei informiert, wird angezeigt.
7. Verteilen Sie die virtuelle Client-Datei `recoverytoken.tok` an die betreffenden SafeGuard Enterprise Benutzer.

Der Benutzer sollte diese Datei an einem sicheren Speicherort, z. B. auf einem USB-Stick, speichern. Beim Starten eines Challenge/Response-Verfahrens muss diese Datei im selben Verzeichnis wie das Recovery Tool abgelegt sein.

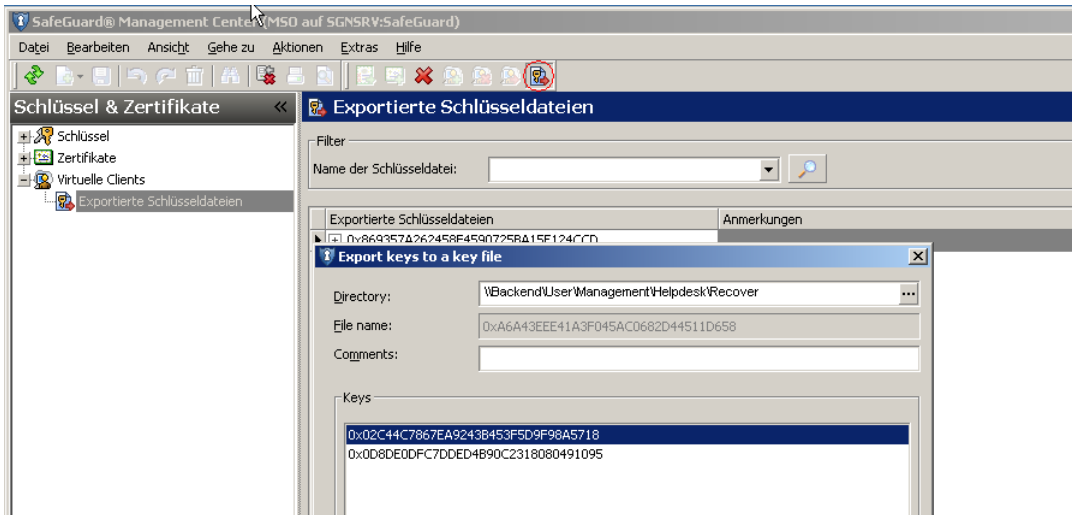
9.3.3 Schlüsseldateien für den Recovery-Vorgang anlegen und exportieren

Sind mehrere Schlüssel erforderlich, um den Zugriff auf ein verschlüsseltes Volume im Rahmen eines Recovery-Verfahrens mit virtuellen Clients wiederherzustellen, so kann der Sicherheitsbeauftragte diese Schlüssel in einer exportierten Schlüsseldatei zusammenfassen. Diese Schlüsseldatei wird mit einem Zufallskennwort verschlüsselt, das in der Datenbank gespeichert wird. Das Kennwort ist für jede angelegte Schlüsseldatei einzigartig.

Die verschlüsselte Schlüsseldatei muss an den Benutzer übertragen werden und ihm beim Starten eines Challenge/Response-Verfahrens über ein Recovery Tool zur Verfügung stehen.

Im Rahmen des Challenge/Response-Verfahrens wird das Kennwort für die Schlüsseldatei mit dem Response-Code übertragen. Die Schlüsseldatei kann daraufhin mit dem Kennwort entschlüsselt werden und es besteht wieder Zugriff auf alle Volumes, die mit den verfügbaren Schlüsseln verschlüsselt sind.

1. Öffnen Sie das SafeGuard Management Center und klicken Sie auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite zunächst auf **Virtuelle Clients** und dann auf **Exportierte Schlüsseldateien**.



3. Klicken Sie in der Symbolleiste auf **Neue exportierte Schlüsseldatei**.

4. Geben Sie im Dialog **Schlüssel in eine Schlüsseldatei exportieren** folgende Informationen ein:
   - **Verzeichnis:** Klicken Sie auf **[...]**, um einen Speicherort für die Schlüsseldatei auszuwählen.
   - **Dateiname:** Die Schlüsseldatei ist mit einem Zufallskennwort verschlüsselt, das hier angezeigt wird. Sie können den hier angezeigten Namen nicht ändern.
   - Klicken Sie auf **Schlüssel hinzufügen** oder **Schlüssel entfernen**, um Schlüssel hinzuzufügen oder zu entfernen. Ein Popupfenster, in dem Sie nach den gewünschten Schlüsseln suchen und diese auswählen können, wird angezeigt. Bestätigen Sie Ihre Auswahl mit **OK**.
   - Klicken Sie auf **OK**, um Ihre Angaben zu bestätigen.
5. Verteilen Sie diese Schlüsseldatei an die betreffenden Benutzer. Sie muss den Benutzern vor der Eingabe des Response-Codes auf Client-Seite zur Verfügung stehen.

9.3.4 Virtuelle Clients anzeigen und Ansicht filtern

Um Ihnen das Auffinden des erforderlichen virtuellen Clients oder Schlüssels während eines Challenge/Response-Verfahrens zu erleichtern, bietet der Bereich **Schlüssel & Zertifikate** des SafeGuard Management Centers verschiedene Filter- und Suchfunktionalitäten.

Ansichten für virtuelle Clients

1. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
2. Klicken Sie auf das Lupensymbol, um eine vollständige Liste aller virtuellen Clients zu erstellen.
3. Filtern Sie die virtuellen Clients nach **Symbolischer Name** oder **Schlüssel-GUID**.

Ansichten für exportierte Schlüsseldateien

1. Klicken Sie auf **Virtuelle Clients** und dann auf **Exportierte Schlüsseldateien**.
2. Klicken Sie auf das Lupensymbol, um eine vollständige Liste aller exportierten Schlüsseldateien zu erstellen.
3. Klicken Sie auf das + Symbol neben der gewünschten Schlüsseldatei, um die in der Datei enthaltenen Schlüssel anzuzeigen.

9.3.5 Virtuelle Clients löschen

So löschen Sie einen virtuellen Client:

1. Öffnen Sie das SafeGuard Management Center und klicken Sie auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
3. Suchen Sie im Aktionsbereich nach dem entsprechenden virtuellen Client, indem Sie auf das Lupensymbol klicken. Die verfügbaren virtuellen Clients werden angezeigt.
4. Wählen Sie den gewünschten Eintrag im Aktionsbereich aus und klicken Sie in der Symbolleiste auf **Virtuellen Client löschen**.
5. Speichern Sie ihre Änderungen in der Datenbank, indem Sie in der Symbolleiste auf das Symbol **Speichern** klicken.

Der virtuelle Client wird aus der Datenbank gelöscht.

10 Mit Richtlinien arbeiten

Die folgenden Abschnitte beschreiben richtlinienrelevanten Vorgänge, z. B. das Erstellen, Gruppieren und Sichern von Richtlinien.

Alle mit SafeGuard Enterprise verfügbaren Richtlinieneinstellungen sind unter *Sicherheitsrichtlinien* beschrieben.

10.1 Richtlinien anlegen

So legen Sie eine neue Richtlinie an:

1. Melden Sie sich mit dem Kennwort, das Sie während der Erstkonfiguration festgelegt haben, am SafeGuard Management Center an.
2. Klicken Sie auf die Schaltfläche **Richtlinien** im Navigationsbereich.
3. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf **Richtlinien** und wählen Sie im Kontextmenü den Befehl **Neu**.
4. Wählen Sie den Richtlinientyp aus. Es wird ein Dialog für die Benennung der Richtlinie des ausgewählten Richtlinientyps angezeigt.
5. Geben Sie einen Namen und optional eine Beschreibung für die Richtlinie ein.

   Richtlinien für den Geräteschutz:

   Wenn Sie eine Richtlinie für den Geräteschutz anlegen wollen, müssen Sie in diesem Dialog auch das Ziel des Geräteschutzes angeben. Mögliche Ziele sind:

- Massenspeicher (Boot-Laufwerke/Andere Volumes)
- Wechselmedien
- Optische Laufwerke

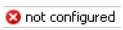
  Für jedes Ziel muss eine eigene Richtlinie angelegt werden. Sie können die einzelnen Richtlinien später z. B. zu einer Richtliniengruppe mit der Bezeichnung *Verschlüsselung* zusammenfassen.

6. Klicken Sie auf **OK**.

Die neu angelegte Richtlinie wird im Navigationsfenster unter **Richtlinien** angezeigt. Im Aktionsbereich werden alle Einstellungen für den gewählten Richtlinientyp angezeigt.

10.2 Richtlinieneinstellungen bearbeiten

Wenn Sie im Navigationsfenster eine Richtlinie auswählen, können Sie deren Einstellungen im Aktionsbereich bearbeiten.

	Das rote Symbol vor dem Text „nicht konfiguriert“ gibt an, dass für diese Einstellung ein Wert festgelegt werden muss. Sie können die Richtlinie erst speichern, wenn Sie eine andere Einstellung als „nicht konfiguriert“ ausgewählt haben.

10.2.1 Einstellungen auf Standardwerte setzen

In der Symbolleiste stehen folgende Symbole für Richtlinieneinstellungen zur Verfügung:

	Zeigt die Standardwerte für nicht konfigurierte Richtlinieneinstellungen.
	Setzt die markierte Richtlinieneinstellung auf „nicht konfiguriert”.
	Setzt alle Richtlinieneinstellungen eines Bereichs auf „nicht konfiguriert”.
	Setzt den Standardwert für die markierte Richtlinieneinstellung.
	Setzt alle Richtlinieneinstellungen eines Bereichs auf den Standardwert.

10.2.2 Maschinen- und benutzerspezifische Richtlinien unterscheiden

Richtlinienfarbe blau	Richtlinie wird nur für Maschinen angewandt, nicht für Benutzer.
Richtlinienfarbe schwarz	Richtlinie wird für Maschinen und Benutzer angewandt.

10.3 Richtliniengruppen

SafeGuard Enterprise Richtlinien müssen in Richtliniengruppen zusammengefasst werden. Eine Richtliniengruppe kann verschiedene Richtlinientypen enthalten.

Wenn Sie Richtlinien vom selben Typ in einer Gruppe zusammenfassen, werden die Einstellungen automatisch vereinigt. Sie können dafür eine Auswertungsreihenfolge festlegen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten. Ist eine Einstellung auf **nicht konfiguriert** gesetzt, wird die Einstellung in einer niedriger priorisierten Richtlinie **nicht überschrieben**.

Ausnahme Geräteschutz:

Richtlinien für den Geräteschutz werden nur vereinigt, wenn sie für dasselbe Ziel (z. B. Boot-Volume) angelegt werden. Weisen sie auf verschiedene Ziele, werden sie addiert.

10.3.1 Richtlinien zu Gruppen zusammenfassen

Die einzelnen Richtlinien der verschiedenen Typen müssen angelegt sein.

So fassen Sie Richtlinien zu Gruppen zusammen:

1. Klicken Sie auf die Schaltfläche **Richtlinien** im Navigationsbereich.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste **Richtlinien-Gruppen** und wählen Sie **Neu**.
3. Klicken Sie auf **Neue Richtlinien-Gruppe**. Es wird ein Dialog für die Benennung der Richtlinien-Gruppe angezeigt.
4. Geben Sie einen eindeutigen Namen und optional eine Beschreibung für die Richtlinien-Gruppe ein. Klicken Sie auf **OK**.
5. Die neu angelegte Richtlinie-Gruppe wird im **Navigationsfenster** unter **Richtlinien-Gruppen** angezeigt.
6. Wählen Sie die Richtlinien-Gruppe aus. Im Aktionsbereich werden alle für das Gruppieren der Richtlinien notwendigen Elemente angezeigt.
7. Zum Gruppieren der Richtlinien ziehen Sie sie aus der Liste der verfügbaren Richtlinien in den Richtlinienbereich.
8. Sie können für jede Richtlinie eine **Priorität** festlegen, indem Sie die Richtlinie über das Kontextmenü nach oben oder unten reihen.

Wenn Sie Richtlinien vom selben Typ in einer Gruppe zusammenfassen, werden die Einstellungen automatisch vereinigt. Sie können dafür eine Auswertungsreihenfolge festlegen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten. Ist eine Einstellung auf **nicht konfiguriert** gesetzt, wird die Einstellung in einer niedriger priorisierten Richtlinie **nicht überschrieben**.

Ausnahme Geräteschutz:

Richtlinien für den Geräteschutz werden nur vereinigt, wenn sie für dasselbe Ziel (z. B. Boot-Volume) angelegt werden. Weisen sie auf verschiedene Ziele werden sie addiert.

9. Speichern Sie die Richtliniengruppe über **Datei > Speichern**.

Die Richtliniengruppe enthält nun die Einstellungen aller einzelnen Richtlinien.

10.3.2 Ergebnis der Gruppierung

Das Ergebnis der Zusammenfassung wird in einer eigenen Ansicht dargestellt.

Klicken Sie zum Anzeigen der Zusammenfassung auf die Registerkarte **Ergebnis**.

- Für jeden Richtlinien-Typ steht eine eigene Registerkarte zur Verfügung.

  Die aus der Zusammenfassung der einzelnen Richtlinien resultierenden Einstellungen werden angezeigt.

- Für Richtlinien zum Geräteschutz werden Registerkarten für jedes Ziel der Richtlinie angezeigt (z. B. Boot-Volumes, Laufwerk X: usw.).

10.4 Richtlinien und Richtliniengruppen sichern

Sie können Sicherungskopien von Richtlinien und Richtliniengruppen in Form von XML-Dateien erstellen. Falls notwendig, lassen sich die betreffenden Richtlinien/Richtliniengruppen daraufhin aus diesen XML-Dateien wiederherstellen.

So erstellen Sie eine Sicherungskopie von einer Richtlinie/Richtliniengruppe:

1. Markieren Sie die Richtlinie/Richtliniengruppe im Navigationsfenster unter **Richtlinien** bzw. **Richtlinien-Gruppen**.
2. Klicken Sie mit der rechten Maustaste und wählen Sie im angezeigten Kontextmenü **Richtlinie sichern**.

Der Befehl **Richtlinie sichern** steht auch im Menü **Aktionen** zur Verfügung.

3. Geben Sie im Dialog **Speichern unter** einen Dateinamen für die XML-Datei an und wählen Sie das Verzeichnis, in dem die Datei gespeichert werden soll, aus. Klicken Sie auf **Speichern**.

Die Sicherungskopie der Richtlinie/Richtliniengruppe ist im angegebenen Verzeichnis als XML-Datei abgelegt.

10.5 Richtlinien und Richtliniengruppen wiederherstellen

So stellen Sie eine Richtlinie/Richtliniengruppe aus einer XML-Datei wieder her:

1. Markieren Sie im Navigationsbereich **Richtlinien/Richtlinien-Gruppen**.
2. Klicken Sie mit der rechten Maustaste und wählen Sie im angezeigten Kontextmenü **Richtlinie wiederherstellen**.

   Der Befehl **Richtlinie wiederherstellen** steht auch im Menü **Aktionen** zur Verfügung.
3. Wählen Sie die XML-Datei für die Wiederherstellung der Richtlinie/Richtliniengruppe aus und klicken Sie auf **Öffnen**.

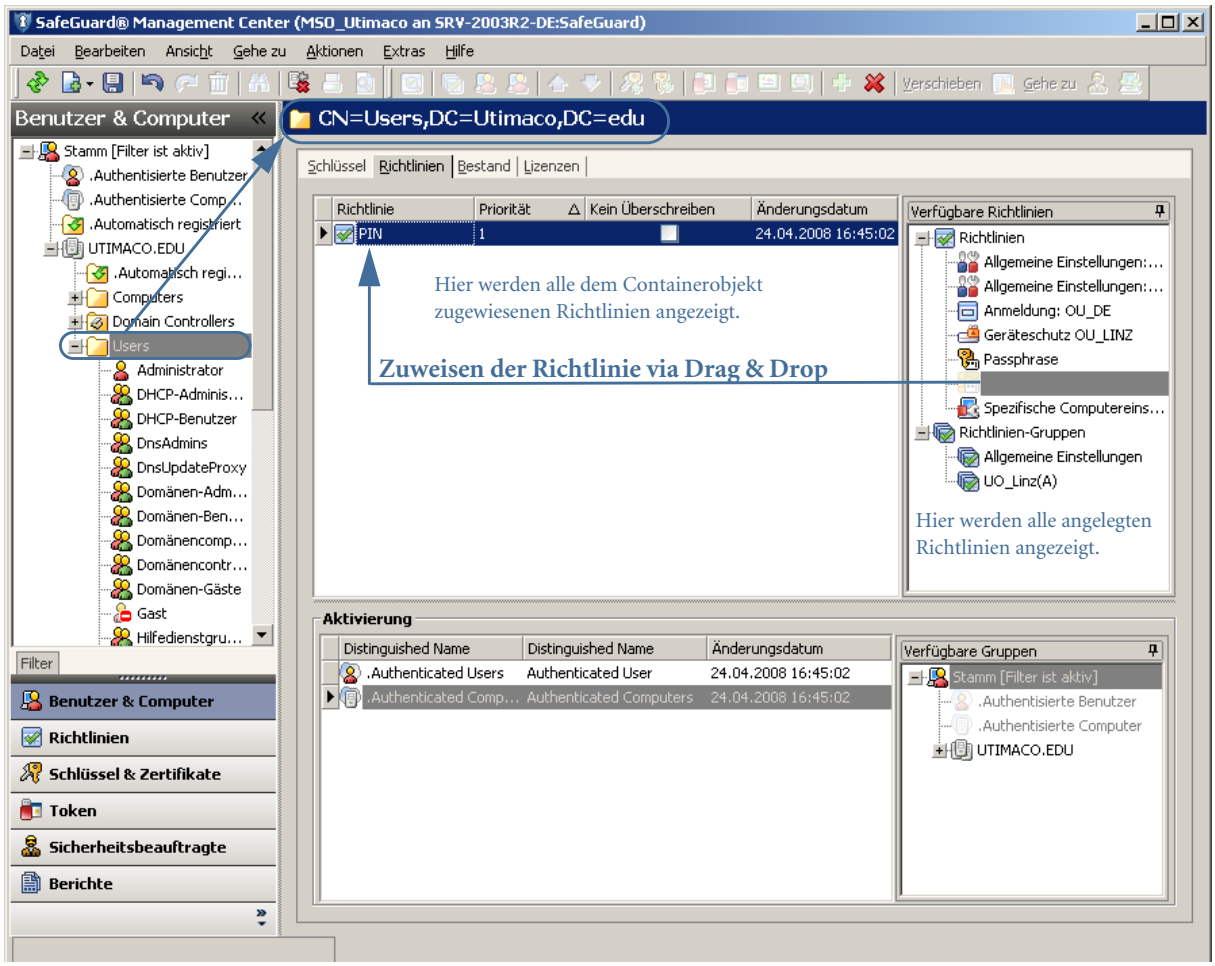
Die Richtlinie/Richtliniengruppe ist wiederhergestellt.

10.6 Richtlinien zuweisen

So weisen Sie Richtlinien zu:

1. Klicken Sie auf **Benutzer & Computer**. Wählen Sie das Container-Objekt (z. B. OU oder Domäne) im Navigationsfenster aus. Klicken Sie - falls notwendig - auf die Registerkarte **Richtlinien**.

   Im Aktionsbereich werden alle für die Zuweisung der Richtlinie notwendigen Elemente angezeigt.

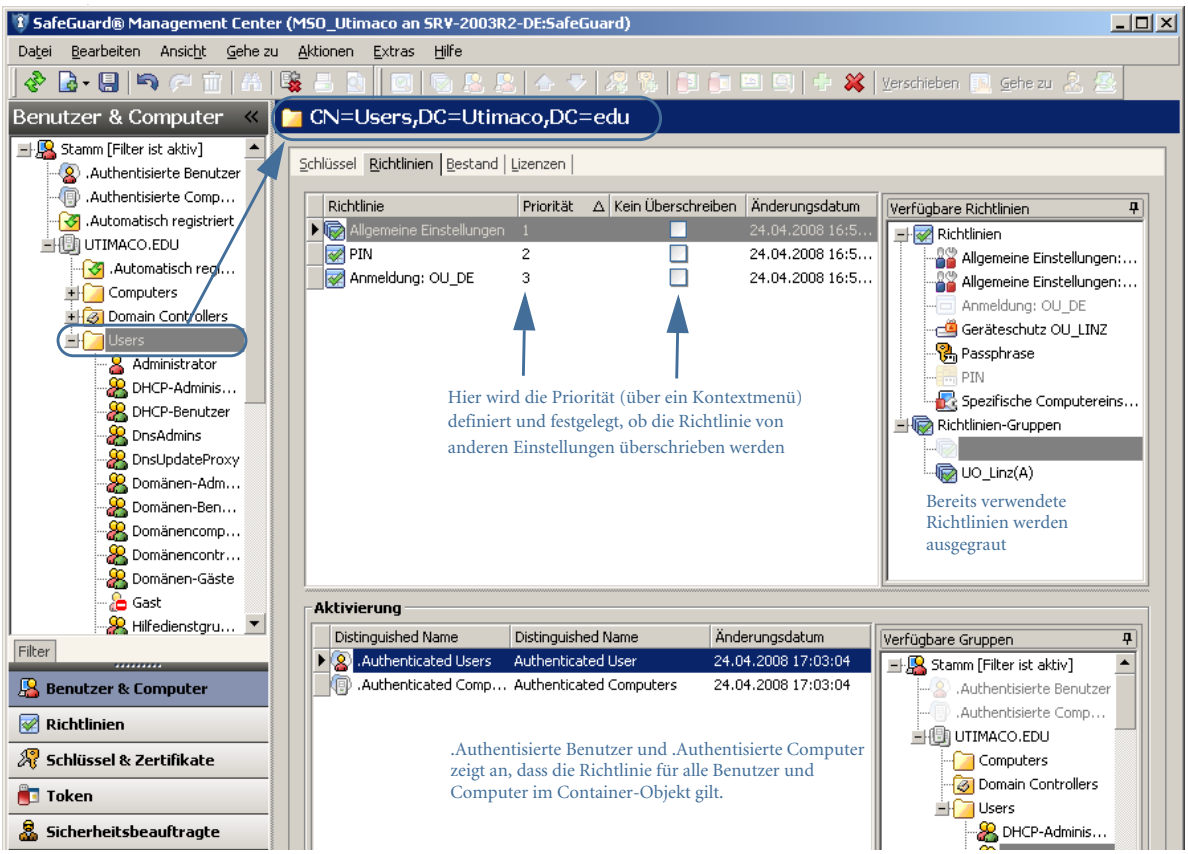


2. Zum Zuweisen einer Richtlinie ziehen Sie sie aus der Liste der verfügbaren Richtlinien in den Richtlinienbereich.

3. Sie können für jede Richtlinie eine **Priorität** festlegen, indem Sie die Richtlinie über das Kontextmenü nach oben oder unten reihen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten.

   Wenn Sie für eine Richtlinie **Kein Überschreiben** aktivieren, können die Einstellungen dieser Richtlinie nicht von anderen überschrieben werden.

Hinweis: Wenn Sie bei einer Richtlinie mit niedrigerer Priorität die Option**Kein Überschreiben** aktivieren, so zieht diese Richtlinie, trotz niedrigerer Priorität gegenüber einer Richtlinie mit einer höheren Priorität.



4. Im Aktivierungsbereich werden die Gruppen .Authentisierte Benutzer - bzw. Computer angezeigt.

Die Richtlinie gilt jetzt für alle Gruppen innerhalb der OU bzw. Domäne.

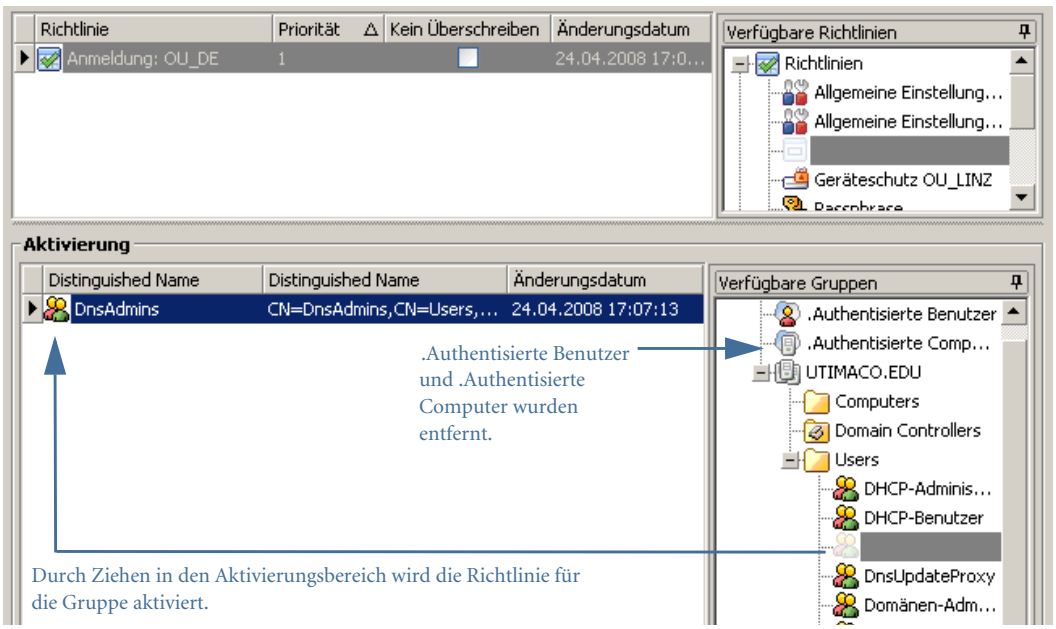
10.6.1 Richtlinien für einzelne Gruppen aktivieren

Richtlinien werden immer einer OU bzw. einer Domäne oder Arbeitsgruppe zugewiesen. Sie gelten standardmäßig für alle Gruppen in diesen Container-Objekten (die Gruppen .Authentisierte Benutzer und .Authentisierte Computer werden im Aktivierungsbereich angezeigt).

Sie können aber auch Richtlinien festlegen und sie für eine einzelne oder mehrere Gruppen aktivieren. Diese Richtlinien gelten dann ausschließlich für diese Gruppen.

Gehen Sie zum Festlegen einer Richtlinie, die nur für eine bestimmte Gruppe gelten soll, folgendermaßen vor:

1. Weisen Sie die Richtlinie der OU, in der sich die Gruppe befindet, zu.
2. Im Aktivierungsbereich werden die Gruppen .Authentisierte Benutzer und .Authentisierte Computer angezeigt.
3. Ziehen Sie diese beiden Gruppen aus dem Aktivierungsbereich in die Liste der verfügbaren Gruppen.
   Die Richtlinie ist in dieser Konstellation für keinen Benutzer und keinen Computer wirksam.
4. Ziehen Sie jetzt die gewünschte Gruppe (oder auch mehrere Gruppen) aus der Liste der verfügbaren Gruppen in den Aktivierungsbereich.



Diese Richtlinie gilt jetzt ausschließlich für diese Gruppe.

Wurden der übergeordneten OU ebenfalls Richtlinien zugeordnet, gilt diese Richtlinie für diese Gruppe zusätzlich zu jenen, die für die gesamte OU festgelegt wurden.

10.7 Übertragung von Richtlinien deaktivieren

Um die Übertragung von Richtlinien an dieEndpoint-Computer zu deaktivieren, stehen in der SafeGuard Management Center Symbolleiste die Schaltfläche **Richtlinienverteilung aktivieren/deaktivieren** sowie im Menü **Bearbeiten** der Befehl **Richtlinienverteilung aktivieren/deaktivieren** zur Verfügung. Wenn Sie auf diese Schaltfläche klicken, den Befehl auswählen oder F3 drücken, werden keine Richtlinien an die Endpoint-Computer gesendet. Durch erneutes Klicken auf die Schaltfläche und Auswählen des Befehls oder Drücken der F3-Taste wird die Deaktivierung wieder aufgehoben.

Hinweis: Um die Übertragung von Richtlinien zu deaktivieren, benötigen Sie als Sicherheitsbeauftragter die Berechtigung „Richtlinienverteilung aktivieren/deaktivieren“. Den beiden vordefinierten Rollen Haupt-Sicherheitsbeauftragter und Sicherheitsbeauftragter ist diese Berechtigung standardmäßig zugewiesen. Neu angelegten benutzerdefinierten Rollen kann diese Berechtigung jederzeit zugewiesen werden.

10.8 Regeln für die Zuweisung und Auswertung von Richtlinien

Die Verwaltung und Auswertung von Richtlinien folgt den in diesem Kapitel dargestellten Regeln.

10.8.1 Richtlinien zuweisen und aktivieren

Damit eine Richtlinie für einen Benutzer/Computer wirksam werden kann, muss sie einem Container-Objekt (Root-Knoten, Domäne, OU, BuiltIn-Container oder Arbeitsgruppe) zugewiesen werden. Damit die zugewiesene Richtlinie für Benutzer/Computer wirksam wird, werden beim Zuweisen einer Richtlinie an einer beliebigen Stelle in der Hierarchie alle Computer (authentisierte Computer) und alle Benutzer (authentisierte Benutzer) automatisch aktiviert (die alleinige Zuweisung ohne Aktivierung reicht nicht aus). In diesen Gruppen sind alle Benutzer bzw. Computer zusammengefasst.

10.8.2 Vererbung von Richtlinien

Vererbung von Richtlinien ist nur zwischen Container-Objekten möglich. Nur Container-Objekte können Richtlinien von übergeordneten Container-Objekten erben. Innerhalb eines Containers - vorausgesetzt er enthält keine weiteren Container-Objekte - können Richtlinien nur aktiviert werden (auf Gruppenebene). Vererbung zwischen Gruppen ist nicht möglich.

10.8.3 Vererbungsreihenfolge von Richtlinien

Werden Richtlinien entlang einer Hierarchiekette zugewiesen, so wirkt jene Richtlinie am stärksten, die näher beim Zielobjekt (Benutzer/Computer) ist. Das bedeutet: mit der Entfernung zum Zielobjekt verliert die Richtlinie immer mehr an Kraft - wenn nähere Richtlinien vorhanden sind.

10.8.4 Direkte und indirekte Zuweisung von Richtlinien

Direkte Zuweisung:

Der Benutzer/Computer erhält eine Richtlinie, die direkt dem Container-Objekt, in dem er sich tatsächlich befindet (Mitgliedschaft alleine reicht nicht aus), zugewiesen wurde. Das Container-Objekt hat diese Richtlinie nicht geerbt!

Indirekte Zuweisung:

Der Benutzer/Computer erhält eine Richtlinie, die das Container-Objekt, in dem er sich tatsächlich befindet (die Mitgliedschaft in einer Gruppe, die sich in einem anderen Container-Objekt befindet, als der Benutzer, reicht nicht aus!), von einem ihr übergeordneten Container-Objekt geerbt hat.

10.8.5 Aktivierung/Deaktivierung von Richtlinien

Damit eine Richtlinie für einen Computer/Benutzer wirken kann, muss diese auf Gruppenebene aktiviert werden (Richtlinien können ausschließlich auf Gruppenebene aktiviert werden). Es spielt keine Rolle, ob sich diese Gruppe im selben Container-Objekt befindet, oder nicht. Wichtig ist hier nur, dass der Benutzer oder Computer eine direkte bzw. indirekte (durch Vererbung) Zuordnung der Richtlinie erhalten hat.

Befindet sich ein Computer oder Benutzer außerhalb einer OU oder Vererbungslinie und ist Mitglied einer Gruppe, die sich innerhalb dieser OU befindet, so gilt diese Aktivierung für diesen Benutzer oder Computer **nicht**. Denn für diesen Benutzer oder Computer ist keine gültige Zuweisung (direkt bzw. indirekt) vorhanden. Die Gruppe wurde zwar aktiviert, aber eine Aktivierung kann nur für Benutzer und Computer gelten, für die es auch eine Richtlinienzuweisung gibt. D. h. die Aktivierung von Richtlinien kann nicht über Container-Grenzen hinausgehen, wenn keine direkte oder indirekte Richtlinienzuweisung für dieses Objekt existiert.

Eine Richtlinie wird wirksam, wenn sie entweder bei Benutzergruppen oder Computergruppen aktiviert wurde. Es werden die Benutzergruppen und dann die Computergruppen ausgewertet (auch authentisierte Benutzer und authentisierte Computer sind Gruppen). Beide Ergebnisse werden ODER-verknüpft. Liefert diese ODER-Verknüpfung einen positiven Wert für die Computer/Benutzer-Beziehung, gilt die Richtlinie.

Hinweis: Werden mehrere Richtlinien für ein Objekt aktiv, werden die einzelnen Richtlinien unter Einhaltung der beschriebenen Regeln, vereinigt. Das heißt, die tatsächlichen Einstellungen für ein Objekt können aus mehreren unterschiedlichen Richtlinien zusammengesetzt werden.

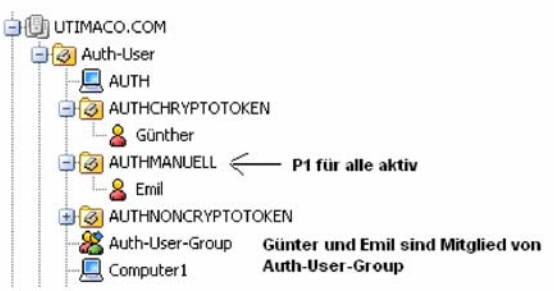
Für eine Gruppe gibt es folgende Aktivierungseinstellungen:

- Aktiviert
  Eine Richtlinie wurde zugewiesen. Die Gruppe wird im Aktivierungsbereich des SafeGuard Management Centers angezeigt.
- Nicht aktiviert
  Eine Richtlinie wurde zugewiesen. Die Gruppe befindet sich nicht im Aktivierungsbereich.

Wird eine Richtlinie einem Container zugewiesen, dann bestimmt die Aktivierungseinstellung für eine Gruppe (aktiviert), ob diese Richtlinie an diesem Container in die Berechnung der resultierenden Richtlinie einfließt.

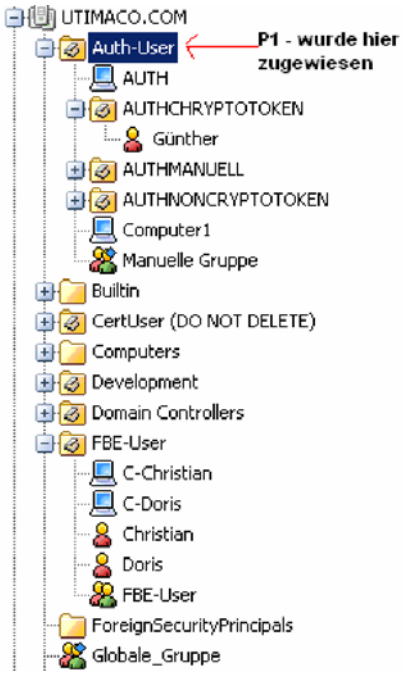
Vererbte Richtlinien können durch diese Aktivierungen nicht kontrolliert werden. Hierfür müsste an der lokaleren OU "Richtlinienvererbung blockieren" gesetzt werden, damit die globalere Richtlinie hier nicht wirken kann.

Beispiel 1:



Es gibt eine gültige Zuweisung der Richtlinie P1 für die OU **AUTHMANUELL** und eine Aktivierung für die Gruppe **Auth-User-Group**. Die Gruppe **Auth-User-Group** hat als Mitglieder die Benutzer Emil und Günther. Obwohl auch der Benutzer Günther Mitglied der Gruppe **Auth-User-Group** ist, gilt die Richtlinie P1 nicht für ihn, sondern nur für den Benutzer Emil. Da es für den Benutzer Günther keine gültige Zuweisung der Richtlinie P1 gibt (Benutzer Günther gehört nicht zur OU **AUTHMANUELL**) hat die Aktivierung der Gruppe **Auth-User-Group** für ihn keine Wirkung.

Beispiel 2



- Struktur des ADs wie rechts
- Richtlinie P1 wird der OU `Auth-User` zugewiesen und wirkt nur für die OU `Auth-User` und deren Sub-OUs
- Richtlinie P1 ist für `Authenticated Users` und für `Authenticated Computer` **NICHT aktiviert**
- Richtlinie P1 ist nur für die Globale Gruppe `Globale_Gruppe` aktiviert (nur der Benutzer `Günther` ist Mitglied dieser Gruppe. Die `Globale_Gruppe` selber ist direkt unter dem Domänenknoten.)

Die Richtlinie P1 wirkt für den Benutzer Günter, da er eine gültige (indirekte) Zuweisung der Richtlinie von der OU `Auth-User` bekommen hat. Dieses Beispiel veranschaulicht, dass die Aktivierung einer Richtlinie an einer beliebigen Stelle im Active Directory gemacht werden kann. Wichtig ist hier nur, dass eine gültige Zuweisung existiert.

10.8.6 Benutzer-/Gruppeneinstellungen

Richtlinieneinstellungen für Benutzer (im SafeGuard Management Center **schwarz** dargestellte Einstellungen), ziehen stärker, als Richtlinieneinstellungen für Computer (im SafeGuard Management Center **blau** dargestellte Einstellungen). Werden bei einer Richtlinie für Computer Benutzereinstellungen durchgeführt, werden diese Einstellungen durch die Richtlinie für den Benutzer überschrieben.

Achtung: Nur die Benutzereinstellungen werden überschrieben. Sollte eine Richtlinie für Benutzer auch Maschineneinstellungen beinhalten (**blau** dargestellte Einstellungen) werden diese nicht von einer Benutzerrichtlinie überschrieben!
Beispiel 1:
Wird für eine Computergruppe die Kennwortlänge 4 definiert, die Benutzergruppe hat aber für dieselbe Einstellung den Wert 3, gilt für diesen Benutzer auf einem Computer der Computergruppe, ein Kennwort mit der Länge 3.
Beispiel 2:
Wird für eine Benutzergruppe ein Serverintervall von 1 Minute definiert und für eine Computergruppe der Wert 3, so wird der Wert 3 verwendet, da es sich beim Wert 1 Minute um eine Maschineneinstellung, die in einer Richtlinie für Benutzer definiert wurde, handelt

10.8.7 Sich widersprechende Verschlüsselungsrichtlinien

Es werden zwei Richtlinien - P1 und P2 - angelegt. Für P1 wurde eine dateibasierende Verschlüsselung für Laufwerk E:\ definiert und für P2 eine volume-basierende Verschlüsselung für Laufwerk E:\. P1 wird der OU **FBE-User** und P2 der OU **VBE-User** zugewiesen.

Fall 1:
Ein Benutzer aus OU **FBE-User** meldet sich zuerst am Client XP-100 (Container Computer) an. Das Laufwerk E:\ wird dateibasierend verschlüsselt. Meldet sich ein Benutzer danach aus der OU **VBE-User** am Client XP-100 an, so wird das Laufwerk E:\ volume-basierend verschlüsselt. Haben beide Benutzer dieselben Schlüssel, können beide auf die Laufwerke bzw. Dateien zugreifen.

Fall 2:
Ein Benutzer aus der OU **VBE-User** meldet sich zuerst am Computer XP-100 (Container Computer) an. Das Laufwerk wird volume-basierend verschlüsselt. Meldet sich nun ein Benutzer der OU **FBE-User** an und hat einen gemeinsamen Schlüssel mit den Benutzern aus der OU **VBE-User**, wird das Laufwerk E:\ (die volume-basierende Verschlüsselung bleibt erhalten) innerhalb der volume-basierenden Verschlüsselung dateibasierende verschlüsselt. Hat der Benutzer aus der OU **FBE-User** allerdings keinen gemeinsamen Schlüssel, kann er auf das Laufwerk E:\ nicht zugreifen.

10.8.8 Priorisierung innerhalb einer Zuweisung

Innerhalb einer Zuweisung, hat die Richtlinie mit der höchsten Priorität (1) Vorrang gegenüber einer Richtlinie mit einer geringeren Priorität.

Achtung: Wurde auf gleicher Ebene eine Richtlinie mit niedriger Priorität, aber mit der Option „Kein Überschreiben“, zugeordnet, so zieht die Richtlinie trotz niedrigerer Priorität gegenüber den Richtlinien mit der höheren Priorität.

10.8.9 Priorisierung innerhalb einer Gruppe

Innerhalb einer Gruppe hat die Richtlinie mit der höchsten Priorität (1) Vorrang gegenüber einer Richtlinie mit einer niedrigeren Priorität.

10.8.10 Statusindikatoren

Durch das Setzen von Statusindikatoren kann das Standardregelwerk der Richtlinien verändert werden.

- **Richtlinienvererbung blockieren**

  Wird direkt bei dem Container gesetzt, der keine übergeordneten Richtlinien empfangen will (Rechtsklick auf das Objekt im Navigationsfenster > Eigenschaften).

- **Kein Überschreiben**

  Wird bei der Zuweisung gesetzt und bedeutet, dass diese Richtlinie nicht von anderen überschrieben werden kann.

Richtlinienvererbung blockieren

Soll ein Container-Objekt keine Richtlinie eines übergeordneten Objektes erben, können Sie das durch das Setzen von „Richtlinienvererbung blockieren“ verhindern. Ist „Richtlinienvererbung blockieren“ gesetzt, werden keine übergeordneten Richtlinieneinstellungen für dieses Container-Objekt wirksam (Ausnahme: „Kein Überschreiben“ wurde bei der Richtlinienzuweisung aktiviert).

Kein Überschreiben

Je weiter die Richtlinienzuweisung mit „Kein Überschreiben“ vom Zielobjekt entfernt ist, umso stärker wird die Wirkung dieser Richtlinie für alle untergeordneten Container-Objekte. Das heißt: „Kein Überschreiben“ eines übergeordneten Containers, überschreibt die Richtlinieneinstellungen eines untergeordneten Containers. So kann z. B. eine Domänenrichtlinie definiert werden, deren Einstellungen nicht überschrieben werden können, auch nicht, wenn für eine OU „Richtlinienvererbung blockieren“ gesetzt wurde!

Achtung: Wurde auf gleicher Ebene eine Richtlinie mit niedriger Priorität, aber mit der Option „Kein Überschreiben“, zugeordnet, so zieht die Richtlinie trotz niedrigerer Priorität gegenüber den Richtlinien mit der höheren Priorität.

10.8.11 Einstellungen in Richtlinien

Computereinstellungen wiederholen

Sie finden diese Einstellung unter:
Richtlinien > Richtlinie vom Typ **Allgemeine Einstellungen** > **Laden der Einstellungen** > **Richtlinien-Loopback**

Wird bei einer Richtlinie vom Typ **Allgemeine Einstellungen** bei der Option **Richtlinien-Loopback** „Computereinstellungen wiederholen“ ausgewählt und die Richtlinie „kommt“ von einem Computer, („Computereinstellungen wiederholen“ hat für eine Benutzerrichtlinie keine Auswirkung) wird diese Richtlinie am Ende der Auswertung noch einmal ausgeführt. Dadurch werden etwaige Benutzereinstellungen wieder überschrieben und es gelten die Computereinstellungen. Für das neuerliche Schreiben, werden sämtliche Computereinstellungen, die der Computer direkt oder indirekt bekommt (auch von Richtlinien die bei Richtlinien-Loopback „Computereinstellungen wiederholen“ nicht gesetzt haben), neu geschrieben.

Benutzer ignorieren

Sie finden diese Einstellung unter:
Richtlinien > Richtlinie vom Typ **Allgemeine Einstellungen** > **Laden der Einstellungen** > **Richtlinien-Loopback**

Wird bei einer Richtlinie vom Typ **Allgemeine Einstellungen** für einen Computer unter dem Richtlinieninhalt **Allgemein** bei der Option Richtlinien-Loopback „Benutzer ignorieren“ ausgewählt und die Richtlinie „kommt“ von einer Maschine, werden nur die Maschineneinstellungen ausgewertet. Benutzereinstellungen werden nicht ausgewertet.

Kein Loopback

Sie finden diese Einstellung unter:
Richtlinien > Richtlinie vom Typ **Allgemeine Einstellungen** > **Laden der Einstellungen** > **Richtlinien-Loopback**

Kein Loopback beschreibt das Standardverhalten. Benutzerrichtlinien gelten vor Computerrichtlinien.

Auswertung der Einstellungen „Benutzer ignorieren“ und „Computereinstellungen wiederholen“

Existieren aktive Richtlinienzuweisungen, werden zuerst die Maschinenrichtlinien ausgewertet und vereinigt. Ergibt diese Vereinigung der einzelnen Richtlinien bei der Option **Richtlinien-Loopback** den Wert „Benutzer ignorieren“, werden die Richtlinien, die für den Benutzer bestimmt gewesen wären, nicht mehr ausgewertet. Das bedeutet sowohl für den Benutzer, als auch für den Computer gelten die gleichen Richtlinien.

Ist nach der Vereinigung der einzelnen Maschinenrichtlinien der Wert bei **Richtlinien-Loopback** „Computereinstellungen wiederholen“, werden die Benutzerrichtlinien mit den Maschinenrichtlinien vereinigt. Nach der Vereinigung, werden die Maschinenrichtlinien nochmals geschrieben und überschreiben gegebenenfalls Einstellungen aus den Benutzerrichtlinien. Ist eine Einstellung in beiden Richtlinien vorhanden, so ersetzt der Wert der Maschinenrichtlinie den Wert der Benutzerrichtlinie.

Ergibt die Vereinigung der einzelnen Maschinenrichtlinien den Standardwert („Kein Richtlinien-Loopback“), so gilt: Benutzereinstellungen vor Maschineneinstellungen.

Ausführungsreihenfolge der Richtlinien

Benutzer ignorieren: Computer

Computereinstellungen wiederholen: Computer -> Benutzer -> Computer
Die erste „Maschinen-Ausführung“ wird für die Richtlinien benötigt, die schon vor der Benutzeranmeldung (z. B. Hintergrundbild bei der Anmeldung) geschrieben werden.

Kein Richtlinien-Loopback (Standardeinstellung): Computer -> Benutzer

10.8.12 Sonstige Definitionen

Die Entscheidung, ob es sich um eine Benutzer- bzw. Maschinenrichtlinie handelt, hängt von der Herkunft der Richtlinie ab. Ein Benutzerobjekt „bringt“ eine Benutzerrichtlinie mit, ein Computer „bringt“ eine Computerrichtlinie mit. Dieselbe Richtlinie kann bei unterschiedlicher Sicht, sowohl Computer- als auch Benutzerrichtlinie sein.

- **Benutzerrichtlinie**

  Jene Richtlinie, die der Benutzer zur Auswertung bereitstellt. Wenn eine Richtlinie nur über einen Benutzer kommt, dann werden die maschinenbezogenen Einstellungen dieser Richtlinie nicht verwendet. Das heißt, es gelten keine computerbezogenen Einstellungen sondern die Standardwerte.

- **Computerrichtlinie**

  Jene Richtlinie, die die Maschine zur Auswertung bereitstellt. Wenn eine Richtlinie nur über einen Computer kommt, dann werden auch die benutzerspezifischen Einstellungen dieser Richtlinie verwendet! Die Computerrichtlinie stellt dann eine „für alle Benutzer" Richtlinie dar.

11 Mit Konfigurationspaketen arbeiten

Im SafeGuard Management Center lassen sich Konfigurationspakete der folgenden Typen erstellen:

- **Konfigurationspakete für zentral verwaltete Computer**

  Computer, die eine Verbindung zum SafeGuard Enterprise Server haben, erhalten Ihre Richtlinien über den Server. Für den erfolgreichen Einsatz der SafeGuard Enterprise Client Software nach der Installation müssen Sie zunächst ein Konfigurationspaket für zentral verwaltete Computer erzeugen und es auf den Computern installieren.

  Nach der ersten Konfiguration der Endpoint-Computer über das Konfigurationspaket erhalten die Computer Richtlinien über den SafeGuard Enterprise Server, wenn Sie diese im Bereich **Benutzer & Computer** des SafeGuard Management Center zugewiesen haben.

- **Konfigurationspakete für Standalone-Computer**

  Standalone-Computer haben niemals eine Verbindung zum SafeGuard Enterprise Server, sie laufen im Standalone-Modus. Die Computer erhalten ihre Richtlinien über Konfigurationspakete. Für den erfolgreichen Einsatz der Software müssen Sie ein Konfigurationspaket mit den relevanten Richtliniengruppen erstellen und es über unternehmenseigene Verteilungsmechanismen an die Endpoint-Computer verteilen. Wenn Richtlinieneinstellungen geändert werden, müssen jeweils neue Konfigurationspakete erstellt und an die Endpoint-Computer verteilt werden.

- **Konfigurationspaket für den SafeGuard Enterprise Server**

  Für den erfolgreichen Einsatz der Software müssen Sie ein Konfigurationspaket für den SafeGuard Enterprise Server erstellen, das die Datenbank sowie die SSL-Verbindung definiert, Scripting API aktiviert, usw.,

Eine detaillierte Beschreibung zum Erstellen der verschiedenen Arten von Konfigurationspaketen finden Sie im SafeGuard Enterprise Installationshandbuch.

Hinweis: Überprüfen Sie Ihr Netzwerk und Ihre Computer in regelmäßigen Abständen auf veraltete oder nicht benutzte Konfigurationspakete und löschen Sie diese aus Sicherheitsgründen. Deinstallieren Sie vor der Installation eines neuen Konfigurationspakets auf dem Computer/ Server jeweils die „alten“ Konfigurationspakete.

12 Administrative Zugangsoptionen für Endpoint-Computer

Für den Fall, dass nach der Installation von SafeGuard Enterprise der Zugang zur Durchführung von administrativen Vorgängen auf Endpoint-Computern erforderlich ist, bietet SafeGuard Enterprise folgende administrative Zugangsoptionen:

- **Service Accounts für die Windows-Anmeldung**

  Mit Service Accounts können sich Benutzer (z. B. Rollout-Beauftragte, Mitglieder des IT-Teams) nach der Installation von SafeGuard Enterprise an Endpoint-Computern anmelden (Windows-Anmeldung), ohne die Power-on Authentication zu aktivieren. Die Benutzer werden auch nicht als SafeGuard Enterprise Benutzer zum Computer hinzugefügt. Service Account Listen werden im Bereich **Richtlinien** des SafeGuard Management Center angelegt und über Richtlinien den Endpoint-Computern zugewiesen. Benutzer, die in eine Service Account Liste aufgenommen wurden, werden bei der Anmeldung am Endpoint-Computer als Gastbenutzer behandelt

Hinweis: Service Account Listen werden den Endpoint-Computern über Richtlinien zugewiesen. Sie sollten bereits im ersten SafeGuard Enterprise Konfigurationspaket, das Sie für die Konfiguration der Endpoint-Computer erstellen, enthalten sein.

Für weitere Informationen zu Service Accounts, siehe *Service Account Listen für die Windows-Anmeldung* auf Seite 97.

- **POA Access Accounts für die POA-Anmeldung an durch SafeGuard Enterprise geschützte Standalone-Computer**

  Für Endpoint-Computer, die im Standalone-Modus laufen, bietet SafeGuard Enterprise POA Access Accounts. POA Access Accounts sind vordefinierte lokale Benutzerkonten, die es Benutzern (z. B. Mitgliedern des IT-Teams) ermöglichen, sich nach der Aktivierung der POA an Endpoint-Computern zur Ausführung administrativer Aufgaben anzumelden. POA Access Accounts ermöglichen die Anmeldung an der POA, eine automatische Anmeldung an Windows erfolgt nicht. Diese Benutzerkonten werden im Bereich **Benutzer & Computer** des SafeGuard Management Center definiert (Benutzer-ID und Kennwort) und werden den Endpoint-Computer über POA-Gruppen in Konfigurationspaketen zugewiesen.

  Für detaillierte Informationen zu POA Access Accounts, siehe *POA Access Accounts für die POA-Anmeldung an Standalone-Computern* auf Seite 103

13 Service Account Listen für die Windows-Anmeldung

Bei den meisten Implementationen von SafeGuard Enterprise installiert zunächst ein Rollout-Team neue Computer in einer Umgebung. Danach folgt die Installation von SafeGuard Enterprise. Zu Installations- und Prüfungszwecken meldet sich der Rollout-Beauftragte dann am jeweiligen Computer an, bevor der Endbenutzer diesen erhält und die Möglichkeit hat, die Power-on Authentication zu aktivieren.

So ergibt sich folgendes Szenario:

1. SafeGuard Enterprise wird auf einem Computer installiert.
2. Nach dem Neustart des Computers meldet sich der Rollout-Beauftragte an.
3. Der Rollout-Beauftragte wird zur POA hinzugefügt und die POA wird aktiv.

Wenn der Endbenutzer den Computer erhält, kann er sich nicht an der POA anmelden und muss ein Challenge/Response-Verfahren durchführen.

Um zu verhindern, dass administrative Vorgänge auf einem durch SafeGuard Enterprise geschützten Computer bewirken, dass die Power-on Authentication aktiviert wird und Rollout-Beauftragte als Benutzer zum Computer hinzugefügt werden, ermöglicht SafeGuard Enterprise das Anlegen von Listen mit Service Accounts. Die in den Listen enthaltenen Benutzer werden dadurch auf den betreffenden Computern als SafeGuard Enterprise Gastbenutzer behandelt.

Mit Service Accounts ergibt sich folgendes Szenario:

1. SafeGuard Enterprise wird auf einem Computer installiert.
2. Der Computer wird neu gestartet und ein Rollout-Beauftragter, der in einer Service Account Liste aufgeführt ist, meldet sich an (Windows-Anmeldung).
3. Gemäß der auf den Computer angewendeten Service Account Liste wird der Benutzer als Service Account erkannt und als Gastbenutzer behandelt.

Der Rollout-Beauftragte wird nicht zur POA hinzugefügt und die POA wird nicht aktiviert. Der Endbenutzer kann sich anmelden und die POA aktivieren.

Hinweis: Service Account Listen sollten bereits im ersten SafeGuard Enterprise Konfigurationspaket, das Sie für die Konfiguration der Endpoint-Computer erstellen, enthalten sein.

13.1 Service Account Listen anlegen und Benutzer hinzufügen

So legen Sie Service Account Listen an und fügen Benutzer hinzu:

1. Klicken Sie auf **Richtlinien** im Navigationsbereich.
2. Markieren Sie **Service Account Listen** im Richtlinien-Navigationsfenster.
3. Klicken Sie im Kontextmenü von **Service Account Listen** auf **Neu > Service Account Liste**.
4. Geben Sie einen Namen für die Service Account Liste ein und klicken Sie auf **OK**.
5. Markieren Sie die neue Liste unter **Service Account Listen** im Richtlinien-Navigationsfenster.
6. Klicken Sie im Aktionsbereich mit der rechten Maustaste, um das Kontextmenü für die Service Account Liste zu öffnen. Wählen Sie **Hinzufügen** im Kontextmenü.
7. Klicken Sie im Arbeitsbereich mit der rechten Maustaste. Das Kontextmenü für die Service Account Liste wird geöffnet. Wählen Sie **Hinzufügen**.
8. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern**-Symbol in der Symbolleiste klicken.

Die Service Account Liste ist registriert und kann beim Anlegen einer Richtlinie ausgewählt werden.

13.2 Zusätzliche Informationen zur Eingabe von Benutzer- und Domänennamen

Für die Definition von Benutzern in Service Account Listen in den beiden Feldern **Benutzername** und **Domänenname** gibt es unterschiedliche Vorgehensweisen(siehe *Verschiedene Anmeldekombinationen abdecken*, Seite 98). Darüber hinaus gelten für die Eingabewerte in diesen Feldern bestimmte Einschränkungen (siehe *Einschränkungen*, Seite 100).

13.2.1 Verschiedene Anmeldekombinationen abdecken

Durch die beiden separaten Felder **Benutzername** und **Domänenname** pro Listeneintrag bieten die Service Account Listen die zum Abdecken aller möglichen Anmeldekombinationen (z. B. „Benutzer@Domäne oder „Domäne\Benutzer“) erforderliche Flexibilität.

Um mehrere Kombinationen aus Benutzername und Domänenname anzugeben, können Sie Asterisken (*) als Platzhalter verwenden. Ein * ist als erstes Zeichen, als letztes Zeichen und als einziges Zeichen zulässig.

Zum Beispiel:

- **Benutzername:** Administrator
- **Domänenname:** *

Mit dieser Kombination geben Sie alle Benutzer mit dem Benutzernamen „Administrator“ an, die sich an einem Netzwerk oder an einer beliebigen lokalen Maschine anmelden.

Der vordefinierte Domänenname [LOCALHOST], der in der Dropdownliste des Felds **Domänenname** zur Verfügung steht, steht für die Anmeldung an einer beliebigen lokalen Maschine.

Zum Beispiel:

- **Benutzername:**: "Admin*"
- **Domänenname**: [LOCALHOST]

Mit dieser Kombination geben Sie alle Benutzer an, deren Benutzernamen mit Admin beginnen und die sich an einer beliebigen lokalen Maschine anmelden.

Darüber hinaus können sich Benutzer auf verschiedene Art und Weise anmelden, z. B.:

- Benutzer: test, Domäne: mycompany
- Benutzer: test, Domäne: mycompany.com.

Da Domänenangaben in Service Account Listen nicht automatisch aufgelöst werden, gibt es drei mögliche Methoden für das korrekte Angeben der Domäne:

- Sie wissen genau, wie der Benutzer sich anmelden wird, und geben die Domäne entsprechend exakt ein.
- Sie erstellen mehrere Einträge in der Service Account Liste.
- Sie verwenden Platzhalter, um alle unterschiedlichen Fälle abzudecken (Benutzer: test, Domäne: mycompany*).

Hinweis: Windows verwendet möglicherweise nicht dieselbe Zeichenfolge und kürzt Namen ab. Um dadurch entstehende Probleme zu vermeiden, empfehlen wir, den FullQualifiedName und den Netbios-Namen einzugeben oder Platzhalter zu verwenden.

13.2.2 Einschränkungen

Asterisken sind nur als erstes, letztes und einziges Zeichen zulässig. Beispiele für gültige und ungültige Zeichenfolgen:

- Gültige Zeichenfolgen sind z. B.: admin*, *, *strator, *minis*.
- Ungültige Zeichenfolgen sind z. B.: **, Admin*trator, Ad*minst*.

Darüber hinaus gelten folgende Einschränkungen:

- Das Zeichen ? ist in Benutzernamen nicht zulässig.
- Die Zeichen / \ [ ] : ; | = , + * ? < > " sind in Domänennamen nicht zulässig.

13.3 Service Account Listen bearbeiten und löschen

Als Sicherheitsbeauftragter mit der Berechtigung **Service Account Listen ändern** können Sie Service Account Listen jederzeit bearbeiten oder löschen:

- Um eine Service Account Liste zu bearbeiten, doppelklicken Sie auf der Liste im Richtlinien-Navigationsfenster. Die Service Account Liste wird geöffnet und Sie können Benutzernamen zufügen, löschen oder ändern.
- Um eine Service Account Liste zu löschen, wählen Sie die Liste im Richtlinien-Navigationsfenster aus, öffnen Sie das Kontextmenü und wählen Sie **Löschen**.

13.4 Service Account Liste über Richtlinie zuweisen

So weisen Sie eine Service Account Liste zu:

1. Legen Sie eine Richtlinie vom Typ **Authentisierung** an oder wählen Sie eine bereits vorhandene aus.
2. Wählen Sie unter **Anmeldeoptionen**, die gewünschte Service Account Liste aus der Dropdownliste des Felds **Service Account Liste**.

Hinweis: Die Standardeinstellung dieses Felds ist **[Keine Liste],** d. h. es gilt keine Service Account Liste. Rollout-Beauftragte, die sich nach der Installation von SafeGuard Enterprise an dem Computer anmelden, werden somit nicht als Gastbenutzer behandelt und können die Power-on Authentication aktivieren sowie zum Computer hinzugefügt werden. Um die Zuweisung einer Service Account Liste rückgängig zu machen, wählen Sie die Option **[Keine Liste]**.

3. Speichern Sie Ihre Änderungen, indem Sie auf das Speichern-Symbol in der Symbolleiste klicken.

Sie können die Richtlinie nun an den Endpoint-Computer übertragen, um die Service Accounts auf dem Computer zur Verfügung zu stellen.

Hinweis: Wenn Sie unterschiedliche Service Account Listen in verschiedenen Richtlinien auswählen, die alle nach dem RSOP (Resulting Set of Policies, die für einen bestimmten Computer/eine bestimmte Gruppe geltenden Einstellungen) relevant sind, setzt die Service Account Liste in der zuletzt angewandten Richtlinie alle zuvor zugewiesenen Service Account Listen außer Kraft. Service Account Listen werden nicht zusammengeführt.

13.5 Richtlinie an den Endpoint-Computer übertragen

Service Account Listen sind während der Installation in der Rollout-Phase einer Implementation besonders hilfreich und wichtig. Es wird daher empfohlen, die Service Account Einstellungen unmittelbar nach der Installation an den Endpoint-Computer zu übertragen. Um die Service Account Liste zu diesem Zeitpunkt auf dem Computer zur Verfügung zu stellen, nehmen Sie in das erste Konfigurationspaket, das Sie zur Konfiguration des Computers nach der Installation erstellen, eine Richtlinie vom Typ **Authentisierung** mit den entsprechenden Einstellungen auf.

Sie können die Einstellungen für die Service Account Liste jederzeit ändern. Die Änderungen werden dann wie üblich über den Server an den Endpoint-Computer übertragen.

13.6 Auf einem Endpoint-Computer mit einem Service Account anmelden

Bei der ersten Windows-Anmeldung nach dem Neustart des Endpoint-Computers meldet sich ein Benutzer, der auf einer Service Account Liste aufgeführt ist, an dem Computer als SafeGuard Enterprise Gastbenutzer an. Diese erste Windows-Anmeldung an dieser Maschine löst weder eine ausstehende Aktivierung der Power-on Authentication aus, noch wird durch die Anmeldung der Benutzer zum Computer hinzugefügt. Das SafeGuard Enterprise System Tray Icon zeigt in diesem Fall auch nicht den Balloon Tool Tip „Initialer Benutzerabgleich abgeschlossen“ an.

13.6.1 Anzeige des Service Account Status auf dem Endpoint-Computer

Der Gastbenutzer-Anmeldestatus wird auch über das System Tray Icon angezeigt. Weitere Informationen zum System Tray Icon finden Sie in der SafeGuard Enterprise Benutzerhilfe, Kapitel *System Tray Icon und Balloon-Ausgabe* (Beschreibung des Benutzerstatus-Felds).

13.7 Protokollierte Ereignisse

Die in Zusammenhang mit Service Account Listen durchgeführten Aktionen werden über die folgenden Ereignisse protokolliert:

SafeGuard Management Center

- Service Account Liste <Name> angelegt.
- Service Account Liste <Name> geändert.
- Service Account Liste <Name> gelöscht.

Durch SafeGuard Enterprise geschützter Computer

- Windows-Benutzer <Domäne/Benutzer> hat sich um <Zeit> an Maschine <Domäne/Computer> als SGN Service Account angemeldet.
- Neue Service Account Liste importiert.
- Service Account Liste <Name> gelöscht.

14 POA Access Accounts für die POA-Anmeldung an Standalone-Computern

Für durch SafeGuard Enterprise geschützte Standalone-Computer, d. h. Computer, die nie eine Verbindung zum Server haben und im Standalone-Modus laufen, bietet SafeGuard Enterprise POA Access Accounts. Nach der Installation von SafeGuard Enterprise und der Aktivierung der Power-on Authentication (POA), kann der Zugang zu Endpoint-Computern für administrative Aufgaben notwendig sein. Mit POA Access Accounts können sich Benutzer (z. B. Mitglieder des IT-Teams) zur Durchführung von administrativen Aufgaben an der Power-on Authentication anmelden, ohne ein Challenge/Response-Verfahren durchführen zu müssen. Eine automatische Anmeldung an Windows erfolgt nicht. Die Benutzer müssen sich an Windows mit ihren vorhandenen Windows-Benutzerkonten anmelden.

14.1 POA Access Accounts erstellen

So erstellen Sie POA Access Accounts:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA** den Knoten **POA-Benutzer**.
3. Klicken Sie im **POA-Benutzer** Kontextmenü auf **Neu > Neuen Benutzer erstellen**.

Der Dialog **Neuen Benutzer erstellen** wird angezeigt.

4. Geben Sie im Feld **Vollständiger Name** einen Namen, d. h. den Anmeldenamen, für den neuen POA-Benutzer ein.
5. Optional können Sie eine Beschreibung für den neuen POA-Benutzer eingeben.
6. Geben Sie ein Kennwort für das neue POA Access Account ein und bestätigen Sie es.

Hinweis: Aus Sicherheitsgründen sollte das Kennwort bestimmten Mindest-Komplexitätsanforderungen entsprechen. Zum Beispiel sollte es eine Mindestlänge von 8 Zeichen haben und sowohl aus numerischen als auch alphanumerischen Zeichen bestehen. Ist das hier eingegebene Kennwort zu kurz, so wird eine entsprechende Warnungsmeldung angezeigt.

7. Klicken Sie auf **OK**.

Das neue POA Access Account wird angelegt und der POA-Benutzer (d. h. das POA Access Account) wird unter **POA-Benutzer** im **Benutzer & Computer** Navigationsbereich angezeigt.

14.2 Kennwort für ein POA Access Account ändern

So ändern Sie das Kennwort für ein POA Access Account:

1. Klicken Sie auf **Benutzer & Computer** im Navigationsbereich des SafeGuard Management Center.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA**, **POA-Benutzer** den relevanten POA-Benutzer.
3. Wählen Sie im Kontextmenü des POA-Benutzers den Befehl **Eigenschaften**.

Der Eigenschaftendialog für den POA-Benutzer wird angezeigt.

4. Geben Sie in der Registerkarte **Allgemein** unter **Benutzerkennwort** das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf **OK**.

Für das relevante POA Access Account gilt das neue Kennwort.

14.3 POA Access Accounts löschen

So löschen Sie POA Access Accounts:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA**, **POA-Benutzer** das relevante POA Access Account.
3. Klicken Sie mit der rechten Maustaste auf das POA Access Account und wählen Sie **Löschen** aus dem Kontextmenü.

Das POA Access Account, d. h. der POA-Benutzer, wird gelöscht und nicht mehr im **Benutzer & Computer** Navigationsfenster angezeigt.

Hinweis: Wenn der Benutzer einer oder mehreren POA-Gruppen angehört, wird er auch aus allen Gruppen entfernt. Das POA Access Account steht jedoch noch so lange auf dem Computer zurVerfügung, bis ein neues Konfigurationspaket erstellt und zugewiesen wird. Für weitere Details zu POA-Gruppen, siehe *POA Access Account Gruppen erstellen*, Seite 105. Für weitere Details zum Ändern der POA Access Account Zuweisung, siehe *POA Access Account Zuweisungen auf Endpoint-Computern ändern*, Seite 108.

14.4 POA Access Account Gruppen erstellen

Damit die POA Access Accounts Endpoint-Computern über Konfigurationspakete zugewiesen werden können, müssen sie in Gruppen zusammengefasst werden. Beim Erstellen von Konfigurationspaketen können Sie dann eine POA Access Account Gruppe für die Zuweisung auswählen.

So erstellen Sie POA Access Account Gruppen:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsbereich unter **POA** den Knoten **POA-Gruppen**.
3. Klicken Sie im **POA-Gruppen** Kontextmenü auf **Neu > Neue Gruppe erstellen**.

Der **Neue Gruppe erstellen** Dialog wird angezeigt.

4. Geben Sie im Feld **Vollständiger Name** einen Namen für die neue POA-Gruppe ein.
5. Optional können Sie eine Beschreibung für die neue POA-Gruppe eingeben.
6. Klicken Sie auf **OK**.

Die neue POA Access Account Gruppe wird angelegt und unter **POA-Gruppen** im **Benutzer & Computer** Navigationsbereich angezeigt. Sie können nun Benutzer, d. h. POA Access Accounts, zur Gruppe hinzufügen.

14.5 POA Access Accounts zu Gruppen hinzufügen

So fügen Sie Benutzer, d. h. POA Access Accounts, zu POA Access Account Gruppen hinzu:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA**, **POA-Gruppe** die relevante POA-Gruppe.

Im Aktionsbereich des SafeGuard Management Center auf der rechten Seite wird die **Mitglieder** Registerkarte angezeigt

3. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **Hinzufügen** Symbol (grünes Pluszeichen).

Der **Mitgliedobjekt auswählen** Dialog wird angezeigt

4. Wählen Sie den Benutzer (d. h. das POA Access Account) den Sie zur Gruppe hinzufügen möchten.
5. Klicken Sie auf **OK**.

Das POA Access Account wird zur Gruppe hinzugefügt und in der Registerkarte **Mitglieder** angezeigt.

Hinweis: Sie können POA Access Accounts auch zu einer Gruppe hinzufügen, indem Sie den POA-Benutzer im Navigationsfenster auswählen und die beschriebenen Schritte ausführen. Der einzige Unterschied bei dieser Vorgehensweise besteht darin, dass nach Auswahl des Benutzers die **Mitglied von** Registerkarte im Aktionsbereich angezeigt wird. Diese Registerkarte zeigt die Gruppen, denen der Benutzer zugewiesen wurde. Der grundlegende Workflow ist identisch.

14.6 Mitglieder aus POA Access Account Gruppen entfernen

So entfernen Sie Mitglieder, d. h. POA Access Accounts, aus Gruppen:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer** Navigationsfenster unter **POA**, **POA-Gruppe** die relevante POA-Gruppe.

Im Aktionsbereich des SafeGuard Management Center auf der rechten Seite wird die **Mitglieder** Registerkarte angezeigt.

3. Wählen Sie den Benutzer, den Sie aus der Gruppe entfernen möchten.
4. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **Löschen** Symbol (rotes Kreuzzeichen).

Der Benutzer wird aus der Gruppe entfernt.

Hinweis: Sie können POA Access Accounts aus einer Gruppe entfernen, indem Sie den POA-Benutzer im Navigationsfenster auswählen und die beschriebenen Schritte ausführen. Der einzige Unterschied bei dieser Vorgehensweise besteht darin, dass nach Auswahl des Benutzers die **Mitglied von** Registerkarte im Aktionsbereich angezeigt wird. Diese Registerkarte zeigt die Gruppen, denen der Benutzer zugewiesen wurde. Der grundlegende Workflow ist identisch.

14.7 POA Access Accounts zu Endpoint-Computern zuweisen

So weisen Sie POA Access Accounts Endpoint-Computern über Konfigurationspakete zu:

1. Wählen Sie im SafeGuard Management Center aus dem Menü **Extras** den Befehl **Konfigurationspakete**.
2. Wählen Sie ein vorhandenes Konfigurationspaket aus oder erstellen Sie ein neues.
3. Wählen Sie eine **POA-Gruppe** aus, die sie zuvor im Bereich **Benutzer & Computer** des SafeGuard Management Center erstellt haben.

   Die Standardeinstellung für die POA-Gruppe ist **Keine Gruppe**

   Darüber hinaus steht standardmäßig eine leere Gruppe zur Auswahl zur Verfügung. Diese Gruppe kann dazu verwendet werden, die Zuweisung einer POA Access Account Gruppe auf Endpoint-Computern zu löschen. Für weitere Details siehe *POA Access Accounts auf Endpoint-Computern löschen*, Seite 108.
4. Geben Sie einen Ausgabepfad für die MSI-Datei an.
5. Klicken Sie auf **Konfigurationspaket erstellen**.
6. Installieren Sie das Konfigurationspaketauf den Endpoint-Computern.

Durch die Installation des Konfigurationspakets werden die Benutzer, d. h. die POA Access Accounts, die in der Gruppe enthalten sind, auf den Computern zur POA hinzugefügt. Die POA Access Accounts stehen für die Anmeldung an die POA zur Verfügung.

14.8 POA Access Accounts auf Endpoint-Computern löschen

Sie können POA Access Accounts auf Endpoint-Computern löschen, indem Sie den Computern eine leere POA Access Account Gruppe zuweisen:

1. Wählen Sie im **Tools** Menü des SafeGuard Management Center den Befehl **Konfigurationspakete**
2. Wählen Sie ein vorhandenes Konfigurationspaket aus oder erstellen Sie ein neues.
3. Wählen Sie eine leere **POA-Gruppe**, die sie zuvor im Bereich **Benutzer & Computer** des SafeGuard Management Center angelegt haben, oder die leere POA-Gruppe, die standardäßig unter **Konfigurationspakete** zur Verfügung steht.
4. Geben Sie einen Ausgabepfad für das Konfigurationspaket an.
5. Kicken Sie auf **Konfigurationspaket erstellen**.
6. Verteilen Sie das Konfigurationspaket an die Endpoint-Computer.

Durch Installation des Konfigurationspakets werden alle POA Access Accounts von den Endpoint-Computern entfernt. Somit werden alle relevanten Benutzer aus der POA entfernt.

14.9 POA Access Account Zuweisungen auf Endpoint-Computern ändern

So ändern Sie die Zuweisung von POA Access Accounts auf Endpoint-Computern:

1. Legen Sie einen neue POA Access Account Gruppe an oder ändern Sie eine bestehende Gruppe.
2. Erstellen Sie ein neues Konfigurationspaket und wählen Sie die neue oder modifizierte POA Access Account Gruppe aus.

Die neue POA Access Account Gruppe steht auf dem Endpoint-Computer zur Verfügung. Alle enthaltenen Benutzer werden zur POA hinzugefügt. Die neue Gruppe überschreibt die alte. POA Access Account Gruppen werden nicht miteinander kombiniert.

14.10 Mit POA Access Account am Endpoint-Computer anmelden

So melden Sie sich mit einem POA Access Account an:

1. Schalten Sie den Computer ein.

Der Power-on Authentication Anmeldedialog wird angezeigt.

2. Geben Sie den **Benutzernamen** und das **Kennwort** des vordefinierten POA Access Account ein.

Sie werden nicht automatisch an Windows angemeldet. Der Windows-Anmeldedialog wird angezeigt.

3. Wählen Sie im **Domäne** Feld die Domäne **<POA>**.

4. Melden Sie sich mit Ihrem vorhandenen Windows-Benutzerkonto an Windows an.

15 Sicherheitsrichtlinien

Die SafeGuard Enterprise Richtlinien enthalten alle Einstellungen, die zur Abbildung einer unternehmensweiten Sicherheitsrichtlinie auf den Endpoint-Computern wirksam werden sollen.

Sie können Richtlinien für folgende Bereiche (Richtlinientypen) erstellen:

- **Allgemeine Einstellungen**
  Enthält Einstellungen für z. B. Transferrate, Hintergrundbilder usw.
- **Authentisierung**
  Enthält Einstellungen zum Anmeldemodus, zur Gerätesperre usw.
- **PINs**
  Legt Anforderungen an die verwendeten PINs fest.
- **Kennwörter**
  Legt Anforderungen an die verwendeten Kennwörter fest.
- **Passphrasen**
  Legt Anforderungen für die verwendeten Passphrasen fest. Passphrasen werden bei der Schlüsselerzeugung für den sicheren Datenaustausch mit SafeGuard Data Exchange verwendet.
- **Geräteschutz**
  Enthält Einstellungen für die volume- oder dateibasierende Verschlüsselung (auch Einstellungen für SafeGuard Data Exchange und SafeGuard Portable): Algorithmen, Schlüssel, Daten auf welchen Laufwerken sollen verschlüsselt werden usw.
- **Spezifische Computereinstellungen**
  Enthält Einstellungen zur Power-on Authentication (aktivieren/deaktivieren), zum sicheren Wake On LAN, Anzeigeoptionen usw.
- **Protokollierung**
  Legt fest, welche Ereignisse wo protokolliert werden.
- **Konfigurationsschutz**
  Enthält Einstellungen (erlauben/sperren) für die Verwendung von Ports, Peripheriegeräten (PDAs, Wechselmedien, Druckern usw.)

15.1 Allgemeine Einstellungen

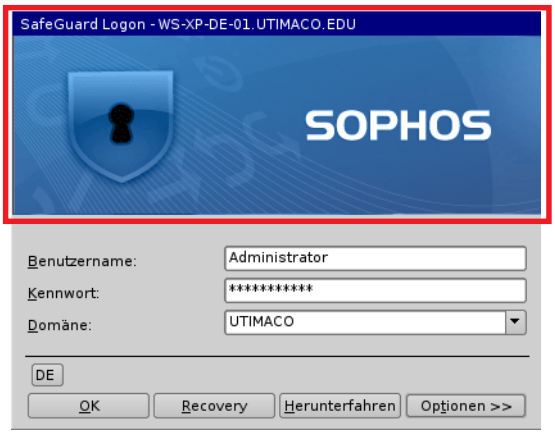
Richtlinieneinstellung	Erklärung
LADEN DER EINSTELLUNGEN	
Richtlinien-Loopback	**Computereinstellungen wiederholen** Wird bei einer Richtlinie unter **Richtlinien-Loopback** ”Computereinstellungen wiederholen” ausgewählt und die Richtlinie ”kommt” von einer Maschine (”Computereinstellungen wiederholen“ einer Benutzer-Richtlinie hat keine Auswirkung), wird diese Richtlinie zum Schluss nochmals ausgeführt. Dadurch werden etwaige Benutzereinstellungen wieder überschrieben und es gelten die Computereinstellungen. **Benutzer ignorieren** Wird bei einer Richtlinie (Maschinen-Richtlinie) unter Richtlinien-Loopback “Benutzer ignorieren” ausgewählt und die Richtlinie "kommt" von einer Maschine, werden nur die Computereinstellungen ausgewertet. Benutzereinstellungen werden nicht ausgewertet. **Kein Loopback** Kein Loopback beschreibt das Standardverhalten: Benutzer-Richtlinien gelten vor Maschinen-Richtlinien. **Wie werden die Einstellungen “Benutzer ignorieren” und “Computereinstellungen wiederholen” ausgewertet?** Existieren aktive Richtlinien-Zuweisungen, werden zuerst die Maschinen-Richtlinien ausgewertet und vereinigt. Ergibt diese Vereinigung der einzelnen Richtlinien beim Attribut **Richtlinien-Loopback** den Wert “Benutzer ignorieren”, so werden Richtlinien, welche für den Benutzer bestimmt gewesen wären, nicht mehr ausgewertet. Das heißt sowohl für den Benutzer wie auch für die Maschine gelten die gleichen Richtlinien. Ist nach der Vereinigung der einzelnen Maschinen-Richtlinien der Wert bei **Richtlinien-Loopback** “Computereinstellungen wiederholen”, werden die Benutzer-Richtlinien mit den Maschinen-Richtlinien vereinigt. Nach der Vereinigung werden die Maschinen-Richtlinien nochmals geschrieben und überschreiben gegebenenfalls Einstellungen aus Benutzer-Richtlinien. Das heißt: Ist eine Einstellung in beiden Richtlinien vorhanden, so ersetzt der Wert der Maschinen-Richtlinie den Wert der Benutzer-Richtlinie.

Richtlinieneinstellung	Erklärung
	Ergibt die Vereinigung der einzelnen Maschinen-Richtlinien den Standardwert, so gilt: Benutzereinstellungen vor Maschineneinstellungen.
TRANSFERRATE	
Server-Verbindungsintervall (in Minuten)	Legt den Zeitraum in Minuten fest, nach dem ein SafeGuard Enterprise Client beim SafeGuard Enterprise Server eine Anfrage nach Richtlinien (-änderungen) stellt. **Hinweis:** Um zu vermeiden, dass eine große Anzahl an Clients gleichzeitig den Server kontaktiert, findet die Kommunikation immer in einem Zeitraum +/- 50% des eingestellten Verbindungsintervalls statt. Beispiel: Die Einstellung “90 Minuten” ergibt einen Kommunikationszeitraum zwischen Client und Server von 45 bis 135 Minuten.
Protokollierung	
Rückmeldung nach Anzahl von Ereignissen	Das Protokollsystem, implementiert als Win32 Service "SGM LogPlayer", sammelt von SafeGuard Enterprise generierte, für die zentrale Datenbank bestimmte Protokolleinträge in lokalen Protokolldateien. Diese befinden sich im LocalCache im Verzeichnis "auditing\SGMTransLog". Diese Dateien werden an den Transportmechanismus übergeben, der sie dann über den SGN Server in die Datenbank einträgt. Die Übergabe erfolgt standardmäßig immer dann, wenn der Transportmechanismus erfolgreich eine Verbindung zum Server aufbauen konnte. Die Größe einer Protokolldatei nimmt also solange zu, bis eine erfolgreiche Verbindung zustande kommt. Um die Größe einer einzelnen Protokolldatei einschränken zu können, kann man über die Richtlinie eine maximale Anzahl von Protokolleinträgen eintragen. Dann wird die Protokolldatei vom Protokollsystem nach Erreichen der eingestellten Anzahl von Einträgen in die Transportqueue des SGN Servers gestellt und eine neue Protokolldatei begonnen.

Richtlinieneinstellung	Erklärung
ANPASSUNG	
Sprache am Client	Legt fest, in welcher Sprache die Einstellungen für SafeGuard Enterprise auf dem Endpoint-Computer angezeigt werden. Neben den unterstützten Sprachen kann auch die Betriebssystem-Spracheinstellung des Endpoint-Computers ausgewählt werden.
RECOVERY FÜR DIE ANMELDUNG	
Recovery für die Anmeldung nach Beschädigung des Windows Local Cache aktivieren	Der Windows Local Cache ist Start- und Endpunkt für den Datenaustausch zwischen Endpoint-Computer und Server. Im Windows Local Cache werdenalle Schlüssel, Richtlinien, Benutzerzertifikate und Audit-Dateien abgelegt. Alle im Local Cache abgelegten Daten sind signiert und können nicht manuell geändert werden. Standardmäßig ist der Recovery-Vorgang für die Anmeldung in diesem Fall deaktiviert, d. h. der Windows Local Cache wird automatisch aus seiner Sicherungskopie wiederhergestellt. In diesem Fall ist kein Challenge/Response-Verfahren für die Reparatur notwendig. Soll die Reparatur des Windows Local Cache explizit über ein Challenge/Response-Verfahren durchgeführt werden soll, setzen Sie dieses Feld auf “JA“.
Local Self Help aktivieren	
Local Self Help aktivieren	Legt fest, ob der Benutzer über Local Self Help an seinem Computer anmelden darf, wenn er das Kennwort vergessen hat. Local Self Help ermöglicht dem Benutzer die Anmeldung durch die Beantwortung einer definierten Anzahl an zuvor festgelegten Fragen in der Power-on Authentication. Somit kann sich der Benutzer im Notfall auch in Situationen, in denen weder eine Telefon- noch eine Internetverbindung zur Verfügung steht, ohne die Durchführung eines Challenge/Response-Verfahrens wieder Zugang zu seinem Computer verschaffen. Mit Local Self Help lassen sich Helpdesk-Aufwände und Kosten reduzieren. **Achtung:** Für die Benutzung von Local Self Help ist es notwendig, dass die automatische Anmeldung an Windows aktiviert ist. Andernfalls funktioniert die Anmeldung über Local Self Help nicht.
Minimale Länge der Antwort	Legen Sie hier die Mindestlänge (in Zeichen) für die Antworten fest, die für Local Self Help auf dem Endpoint-Computer hinterlegt werden.

Richtlinieneinstellung	Erklärung
Willkommenstext unter Windows	Hier können Sie einen individuellen Informationstext angeben, der beim Starten des Local Self Help Assistenten im ersten Dialog angezeigt werden soll. Dieser Text muss zuvor erstellt und registriert werden.
Benutzer dürfen eigene Fragen festlegen	Die für Local Self Help zu beantwortenden Fragen können Sie als zuständiger Sicherheitsbeauftragter zentral vordefinieren und per Richtlinie an die Endpoint-Computer verteilen. Sie können die Benutzer jedoch auch per Richtlinie berechtigen, selbst Fragen zu definieren. Um die Benutzer zur Definition eigener Fragen zu berechtigen, wählen Sie in diesem Feld die Einstellung **JA**.
Challenge / Response (C/R)	
Recovery für die Anmeldung über C/R aktivieren	Legt fest, ob ein Benutzer in der Power-on Authentication (POA) eine Challenge erzeugen darf, um über ein Challenge/Response-Verfahren wieder Zugang zu seinem Computer zu erhalten. **JA:** Benutzer darf Challenge erzeugen. In diesem Fall kann der Benutzer über ein Challenge/Response-Verfahren in Notfällen wieder Zugang zu seinem Computer erhalten. **NEIN:** Benutzer darf keine Challenge erzeugen. In diesem Fall kann der Benutzer im Notfall kein Challenge/Response-Verfahren starten, um wieder Zugang zu seinem Computer zu erhalten.
Automatische Anmeldung an Windows erlauben	Erlaubt dem Benutzer nach einer Authentisierung per Challenge/Response die automatische Anmeldung an Windows. **JA:** Benutzer wird automatisch an Windows angemeldet. **NEIN:** Windows-Anmeldebildschirm erscheint. **Anwendungsfall:** Ein Benutzer hat sein Kennwort vergessen. SafeGuard Enterprise meldet ihn nach Austausch von Challenge und Response ohne SGN-Kennwort am PC an. In diesem Fall wird die automatische Anmeldung an Windows ausgeschaltet und der Windows-Anmeldebildschirm erscheint. Da der Benutzer sein SGN-Kennwort (= Windows-Kennwort) nicht weiß, kann er sich nicht anmelden. Mit “JA” wird eine automatische Anmeldung erlaubt und der Benutzer bleibt nicht im Windows-Anmeldebildschirm stecken.

Richtlinieneinstellung	Erklärung
Informationstext	Zeigt nach dem Starten eines Challenge/Response-Vorgangs in der POA einen Informationstext. Als Informationstext kann hier beispielsweise stehen “Bitte rufen Sie Ihren Support unter der Telefonnummer 01234-56789 an.”. Bevor Sie einen Text angeben können, muss dieser als Textdatei im **Richtlinien-Navigationsbereich** unter **Informationstext** erstellt werden.
BILDER	
	Voraussetzung: Neue Bilder müssen im Management Center im Richtlinien-Navigationsbereich unter Bilder registriert werden. Erst nach der Registrierung sind die Bilder verfügbar. Unterstützte Formate: .BMP, PNG, JPEG Tauscht das blaue Hintergrund-Bitmap mit SafeGuard Enterprise Design gegen ein selbstgewähltes aus. Kunden können hier z. B. das Unternehmens-Logo in der POA verwenden. Maximale Dateigröße für alle Hintergrundbilder: 500 KB
Hintergrundbild in der POA	Auflösung: 1024x768 (VESA-Modus) Farben: keine Einschränkung
Hintergrund-Bild in der POA (niedrige Auflösung)	Auflösung: 640x480 (VGA-Modus) Farben: 16 Farben

Richtlinieneinstellung	Erklärung
	Tauscht das SafeGuard Enterprise-Bitmap aus, das im Anmeldedialog der POA angezeigt wird. Hier kann zum Beispiel das Firmenlogo angezeigt werden. Maximale Dateigröße: 100 KB
Anmeldebild in der POA	Auflösung: 413x140 Pixel Farben: keine Einschränkung
Anmeldebild in der POA (niedrige Auflösung)	Auflösung: 413x140 Pixel Farben: 16
	

15.2 Authentisierung

Wie sich Benutzer an ihrer Arbeitsstation anmelden (mit oder ohne Token), wird in einer Richtlinie vom Typ **Authentisierung** festgelegt.

Richtlinieneinstellung	Erklärung
ZUGRIFF	
Benutzer kann nur von der Festplatte booten	Legt fest, ob Benutzer den PC von Festplatte und/oder anderem Medium starten dürfen. **JA:** Benutzer darf ausschließlich von der Festplatte booten. Die Möglichkeit, den PC mit Diskette oder einem weiteren externen Medium zu starten, wird nicht in der POA angeboten. **NEIN:** Benutzer darf den PC von Festplatte, Diskette oder einem externen Medium (USB, CD usw.) starten.
ANMELDEOPTIONEN	
Anmeldemodus	Legt fest, wie sich ein Benutzer in der POA authentisieren muss. ■ **Benutzername/Kennwort** Der Benutzer darf sich nicht mit einem Token, sondern nur mit Benutzernamen und Kennwort in der POA anmelden. ■ **Token** Der Benutzer darf sich nur mit einem Token oder einer Smartcard in der POA anmelden. Dieses Verfahren bietet eine höhere Sicherheit. Bei der Anmeldung wird der Benutzer aufgefordert, seinen Token einzustecken. Durch den Besitz des Token und der Präsentation der PIN wird die Identität des Benutzers verifiziert. Nach korrekter Eingabe der PIN liest SafeGuard Enterprise automatisch die Daten für die Anmeldung des Benutzers aus.

Richtlinieneinstellung	Erklärung
	Achtung: Beachten Sie, dass Sie sich bei Wahl dieses Anmeldeverfahrens nur mit einem vorher ausgestellten Token anmelden können. Eine Kombination beider Einstellungen ist erlaubt. Um zu prüfen, ob die Anmeldung mit Token reibungslos funktioniert, wählen Sie zunächst beide Einstellungen aus. Erst nach erfolgreicher Token-Anmeldung sollten Sie das Anmeldeverfahren **Benutzername/Kennwort** deaktivieren. ■ **Fingerabdruck** Wählen Sie diese Option, um die Anmeldung mit Lenovo-Fingerabdruck-Leser zu aktivieren. Benutzer, für die diese Richtlinie wirksam ist, können sich mit Fingerabdruck oder Benutzername/Kennwort anmelden. Dieser Vorgang bietet das höchste Maß an Sicherheit. Bei der Anmeldung führt der Benutzer den Finger über den Fingerabdruck-Leser. Wenn der Fingerabdruck erfolgreich erkannt wurde, liest die Power-on Authentication die Anmeldeinformationen des Benutzers und meldet den Benutzer an der Power-on Authentication an. Die Anmeldeinformationen werden dann an Windows übertragen und der Benutzer wird an seinem Computer angemeldet. **Achtung:** Nach Auswahl dieses Anmeldevorgangs kann sich der Benutzer nur mit einem vorher registrierten Fingerabdruck oder mit Benutzername und Kennwort anmelden.

Richtlinieneinstellung	Erklärung
Anmeldeoptionen mit Token	Legt den Typ des Token bzw. der Smartcard fest, der am Benutzer-PC verwendet werden soll. ■ **Nicht kryptographisch** Authentisierung an der POA und an Windows mit Anmeldeinformationen. ■ **Kerberos** Zertifikatsbasierte Authentisierung an der POA und an Windows. Der Sicherheitsbeauftragte stellt ein Zertifikat in einer PKI aus und legt es auf dem Token ab. Dieses Zertifikat wird als Benutzerzertifikat in die SafeGuard Enterprise Datenbank importiert. Falls dort bereits ein automatisch erzeugtes Zertifikat existiert, wird es durch das importierte Zertifikat überschrieben. **Hinweis:** Challenge/Response ist mit einem Token, der Kerberos unterstützt, nicht möglich, da keine Anmeldeinformationen in der POA zur Verfügung stehen, die bei einem Challenge/Response-Verfahren verwendet werden
PIN für automatische Anmeldung mit Token	Geben Sie hier eine Default-PIN an, die dem Benutzer die automatische Anmeldung an der Power-on Authentication mit Token oder Smartcard ermöglicht. Der Benutzer muss den Token bei der Anmeldung einstecken. Daraufhin wird eine automatische Anmeldung an der Power-on Authentication durchgeführt und Windows wird gestartet. PIN-Regeln müssen hier nicht beachtet werden. **Achtung:** ■ Diese Option steht nur dann zur Verfügung, wenn die Option **Token** als **Anmeldemodus** gewählt wurde. ■ Wenn diese Option aktiviert wird, muss bei **Durchgehende Anmeldung an Windows** die Einstellung **Durchgehende Anmeldung deaktivieren** gewählt werden.

Richtlinieneinstellung	Erklärung
Erfolglose Anmeldeversuche dieses Benutzers anzeigen	Zeigt (Einstellung: JA) nach der Anmeldung in der POA und Windows einen Dialog mit Informationen über die letzte fehlgeschlagene Anmeldung (Benutzername/Datum/Zeit) an.
Letzte Benutzeranmeldung anzeigen	Zeigt (Einstellung: JA) nach der Anmeldung in der POA und Windows einen Dialog mit Informationen über die ■ letzte erfolgreiche Anmeldung (Benutzername/Datum/Zeit) ■ letzten Anmeldeinformationen des angemeldeten Benutzers an.
'Erzwungene Abmeldung' bei Sperre der Arbeitsstation deaktivieren	Wenn Benutzer den Endpoint-Computer nur für kurze Zeit verlassen wollen, können Sie den Rechner mittels Klick auf die Schaltfläche **Arbeitsstation sperren** für andere Benutzer sperren und danach mit ihrem Kennwort wieder entsperren. Steht diese Einstellung auf NEIN, dann kann sowohl jener Benutzer, der die Arbeitsstation gesperrt hat, als auch ein Administrator diese Sperre aufheben. Hebt ein Administrator die Sperre auf, so wird der aktuell angemeldete Benutzer zwangsweise abgemeldet. Die Einstellung JA ändert dieses Verhalten. In diesem Fall kann nur der Benutzer die Sperre der Arbeitsstation aufheben. Ein Aufheben der Sperre durch den Administrator und das damit verbundene erzwungene Abmelden des Benutzers ist nicht mehr möglich. **Hinweis:** Diese Einstellung wird nur unter Windows XP wirksam.
Letzte Benutzer/Domänen-Auswahl aktivieren	**JA:** Die POA speichert den Benutzernamen und die Domäne des letzten angemeldeten Benutzers. Benutzer müssen den Benutzernamen also nicht jedesmal eingeben, wenn sie sich anmelden. **NEIN:** Die POA speichert den Benutzernamen und die Domäne des letzten angemeldeten Benutzers nicht.

Richtlinieneinstellung	Erklärung
Durchgehende Anmeldung an Windows	**Hinweis**: Soll der Benutzer in der Lage sein, anderen Benutzern Zugriff auf "seinen" Computer zu gewähren, muss er in der Lage sein, die durchgehende Anmeldung an Windows zu deaktivieren. ■ **Benutzer wählen lassen** Im POA Anmeldedialog kann der Benutzer durch Aktivieren/Deaktivieren dieser Option entscheiden, ob er automatisch an Windows angemeldet werden will oder nicht. ■ **Durchgehende Anmeldung erzwingen** Der Benutzer wird immer automatisch an Windows angemeldet. ■ **Durchgehende Anmeldung deaktivieren** Der Windows Anmeldedialog wird nach der POA-Anmeldung angezeigt und der Benutzer muss sich manuell an Windows anmelden.
Service Account Liste	Um zu verhindern, dass durch administrative Vorgänge auf einem durch SafeGuard Enterprise geschützten Computer die Power-on Authentication aktivert wird und Rollout-Beauftragte als Benutzer zum Computer hinzugefügt werden, bietet SafeGuard Enterprise Service Account Listen für Endpoint-Computer. Die Benutzer auf diesen Listen werden als SafeGuard Enterprise Gastbenutzer behandelt. Damit Sie hier eine Liste auswählen können, müssen Sie diese zunächst im **Richtlinien**-Navigations bereich unter **Service Account Listen** anlegen.

Richtlinieneinstellung	Erklärung
BitLocker-OPTIONEN	
BitLocker Anmeldemodus	Als Anmeldemodus für BitLocker können Sie aus folgenden Optionen auswählen. ■ **TPM:** Der Schlüssel für die Anmeldung wird auf dem TPM-Chip gespeichert. ■ **TPM + PIN:** Der Schlüssel für die Anmeldung wird auf dem TPM-Chip gespeichert und zusätzlich wird eine PIN zur Anmeldung benötigt. Einstellungen für die PIN werden unter PIN und Kennwort vorgenommen. ■ **USB-Stick:** Der Schlüssel für die Anmeldung wird auf einem USB-Stick gespeichert. ■ **TPM + USB-Stick:** Der Schlüssel für die Anmeldung wird auf dem TPM-Chip und auf einem USB-Stick gespeichert. Die Anmeldung kann dann entweder mit TPM-Chip oder USB-Stick erfolgen.
BitLocker Anmeldemodus - Fallback	Für den Fall, dass die Anmeldung fehlschlägt, bietet SafeGuard Enterprise als Fallback-Mechanismus die Anmeldung mit USB-Stick oder die Ausgabe einer Fehlermeldung an. **Hinweis:** Wird *USB-Stick* als Anmeldemodus ausgewählt, wird diese Option nicht angeboten.

Richtlinieneinstellung	Erklärung
TPM Plattform Validierungsprofil	Ist TPM auf dem Endpoint-Computer vorhanden, so lässt sich festlegen, welche Art von TPM-Plattform Validierungsprofil verwendet werden soll. Das TPM-Plattform Validierungsprofil spezifiziert die Maßnahmen, die zum Schutz der BitLocker-Verschlüsselungsschlüssel angewendet werden sollen. Ein TPM-Plattform Validierungsprofil besteht aus einer Reihe von PCR-Indizes (Platform Configuration Register). Microsoft empfiehlt die Verwendung des Default-Profils für die Validierung der TPM-Plattform in Windows Vista, das die folgenden Komponenten absichert: ■ den Verschlüsselungsschlüssel gegen Änderungen am CRTM (Core Root of Trust of Measurement), BIOS sowie an Plattformerweiterungen (PCR 0) ■ Option ROM Code (PCR 2) ■ Master Boot Record (MBR) Code (PCR 4) ■ NTFS Boot Sector (PCR 8) ■ NTFS Boot Block (PCR 9) ■ Boot Manager (PCR 10) ■ BitLocker DE Access Control (PCR 11) **Hinweis:** Diese Option steht nur dann zur Verfügung, wenn *TPM* als Anmeldemodus ausgewählt wurde. Wurde *USB Stick* ausgewählt, ist diese Option nicht verfügbar. Weitere Informationen zum TPM-Plattform Validierungsprofil finden Sie hier: *http://msdn2.microsoft.com/en-us/library/aa376469.aspx*

Richtlinieneinstellung	Erklärung
ERFOLGLOSE ANMELDUNGEN	
Maximalanzahl von erfolglosen Anmeldeversuchen	Bestimmt, wie oft ein Benutzer ohne Folgen bei der Anmeldung einen ungültigen Benutzernamen bzw. ein ungültiges Kennwort eingeben darf. Mit "3" darf der Benutzer beispielsweise dreimal hintereinander seinen Benutzernamen oder sein Kennwort falsch eingeben, beim vierten Mal greift die Einstellung unter "Reaktion auf erfolglose Anmeldungen".
Meldungen zur fehlgeschlagenen Anmeldung in der POA anzeigen	Definiert die Detailebene für Meldungen zu fehlgeschlagenen Anmeldungen: ■ Standard: Zeigt eine kurze Beschreibung an. ■ Verbose (ausführlich): Zeigt detaillierte Informationen an.
Reaktion auf erfolglose Anmeldeversuche	
Computer sperren	Legt fest, ob der PC nach fehlgeschlagenen Anmeldeversuchen gesperrt wird. Die Computersperre kann durch Neustart des PCs und durch Anmeldung eines lokalen Administrators aufgehoben werden. Beachten Sie in diesem Zusammenhang auch die Benutzersperre von Windows.
TOKEN-OPTIONEN	
Aktion bei Verlust des Anmeldestatus des Token	Definiert das Verhalten nach dem Trennen des Token vom PC. Mögliche Aktionen sind: ■ Computer sperren ■ PIN-Dialog anzeigen ■ Keine Aktion
Freigabe des Token erlauben	Bestimmt, ob der Token bei der Anmeldung entsperrt werden darf.

Richtlinieneinstellung	Erklärung
OPTIONEN FÜR SPERRE DES GERÄTS	
Bildschirm nach X Minuten Leerlauf sperren	Bestimmt die Zeit, nach deren Überschreitung ein nicht mehr benutzter Desktop automatisch gesperrt wird. Der Standardwert beträgt 0 Minuten, in diesem Fall erfolgt kein automatisches Schließen.
Bei Entfernung des Token Bildschirm sperren	Bestimmt, ob der Bildschirm gesperrt wird, wenn während einer Arbeitssitzung der Token entfernt wird.
Bildschirm nach dem Fortsetzen sperren	Bestimmt, ob der Bildschirm bei Reaktivierung aus dem Standby-Modus gesperrt wird.

15.3 Liste verbotener PINs für die Verwendung mit Richtlinien anlegen

Für Richtlinien des Typs **PIN** kann eine Liste mit verbotenen PINs angelegt werden. Diese Liste definiert die Zeichenfolgen, die in nicht in PINs verwendet werden dürfen.

Hinweis: In den Listen werden die verbotenen PINs durch einen Leerraum oder einen Zeilenumbruch voneinander getrennt.

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Textdateien beträgt **50 KB**. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden Sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Konvertierung durchgeführt wird, werden Sie durch eine Meldung darüber informiert.

So registrieren Sie die Textdateien:

1. Klicken Sie im Richtlinien-Navigationsbereich mit der rechten Maustaste auf **Informationstext** und wählen Sie **Neu > Text**.
2. Geben Sie im Feld **Textelementname** einen Namen für den anzuzeigenden Text ein.
3. Wählen Sie über die Schaltfläche **[...]** die zuvor erstellte Textdatei aus. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Informationstext** im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Es wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

15.4 Syntaxregeln für PINs

PINs können sowohl Ziffern, Buchstaben als auch Sonderzeichen (wie + - ; etc.) enthalten. Verwenden Sie bei der Vergabe einer neuen PIN jedoch keine Zeichen mit der Kombination ALT + <Zeichen>, da dieser Eingabemodus an der Power-on Authentication nicht zur Verfügung steht. Wie PINs, mit der sich Benutzer am System anmelden, beschaffen sein müssen, wird in Richtlinien vom Typ **PIN** eingestellt.

Achtung: Wenn im SafeGuard Enterprise Management Center Regeln für PINs definiert werden, dann sollten im Active Directory keine Regeln definiert werden.

Richtlinieneinstellung	Erklärung
REGELN	
Mindestlänge der PIN	Zeigt an, aus wie vielen Zeichen eine PIN bei der Änderung durch den Benutzer mindestens bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Maximallänge der PIN	Zeigt an, aus wie vielen Zeichen eine PIN bei der Änderung durch den Benutzer maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Mindestanzahl an Buchstaben Mindestanzahl an Ziffern Mindestanzahl an Symbolen	Mit diesen Einstellungen wird erreicht, dass PINs nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthalten, sondern aus einer Kombination bestehen müssen (z. B. „15blume“ etc.). Diese Einstellung ist nur dann sinnvoll, wenn eine PIN-Mindestlänge definiert ist, die größer 2 ist.
Groß-/Kleinschreibung beachten	Diese Einstellung wird nur bei den Punkten **Liste nicht erlaubter PINs benutzen** und **Benutzername als PIN verboten** wirksam. **Fall 1**: Sie haben in der Liste der verbotenen PINs „Tafel“ eingetragen. Steht die Option **Groß-/Kleinschreibung beachten** auf “JA”, werden zusätzliche Kennwortvarianten wie z. B. „TAFEL“ oder „TaFeL“ nicht akzeptiert und die Anmeldung wird verweigert. **Fall 2:** Der Benutzername für einen Anwender lautet „EMaier“. Steht “Groß-/Kleinschreibung beachten” auf JA und “Mit Benutzernamen identisch” auf ’NEIN, darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. ´emaier´ oder ´eMaiEr´ etc.) als PIN verwenden.

Richtlinieneinstellung	Erklärung
Tastaturzeile verboten	Tastaturzeilen sind „123“ oder „qwe“. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturzeilen beziehen sich nur auf den alphanumerischen Tastaturteil.
Tastaturspalte verboten	Als Tastaturspalten werden eingetippte Zeichenreihen wie „yaq1“, „xsw2“ oder „3edc“ (nicht aber „yse4“, „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als PINs abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Drei oder mehr aufeinanderfolgende Zeichen verboten	Verboten werden mit Aktivierung dieser Option Zeichenketten, ■ die im ASCII-Code aufeinander folgen, sowohl in auf- als auch in absteigender Reihenfolge („abc“; „cba“; „:;<“ etc.). ■ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.
Benutzername als PIN verboten	Bestimmt, ob Benutzername und PIN identisch sein dürfen. **JA:** Benutzer darf seinen Windows-Benutzernamen gleichzeitig als PIN verwenden. **NEIN**: Windows-Benutzername und PIN müssen unterschiedlich sein.
Liste nicht erlaubter PINs benutzen	Bestimmt, ob bestimmte Zeichenfolgen für PINs nicht verwendet werden dürfen. Abgelegt sind die Zeichenfolgen in der Liste der verbotenen PINs (z. B. Datei im Format .txt).

Richtlinieneinstellung	Erklärung
Liste nicht erlaubter PINs	Definiert Zeichenfolgen, die in einer PIN nicht verwendet werden dürfen. Wenn ein Benutzer eine verbotene PIN verwendet, wird eine Fehlermeldung. ausgegeben. **Wichtige Voraussetzung:** Eine Liste (eine Datei) mit verbotenen PINs muss im Management Center unter **Informationstext** im Richtlinien-Navigationsbereich registriert werden. Erst nach der Registrierung ist die Liste verfügbar. Maximale Dateigröße: 50 KB, Unterstütztes Format: Unicode **Nicht erlaubte PINs definieren** In der Liste werden die verbotenen PINs mit einem Leerzeichen oder durch einen neuen Zeilenanfang getrennt. *Wildcard*: An der Position, an der Sie den Zeichentyp „*“ eingeben, können mehrere beliebige Zeichen in der PIN enthalten sein. Beispielsweise wird durch *123* jede Zeichenfolge, die 123 enthält, als PIN verboten. **Achtung:** ■ Wenn Sie nur die Wildcard in die Liste einfügen, können sich Benutzer nach einer erzwungenen PIN-Änderung nicht mehr im System anmelden. ■ Benutzer dürfen auf die Datei keinen Zugriff haben. ■ Die Option **Liste nicht erlaubter PINs benutzen** muss aktiviert sein.
ÄNDERUNGEN	
PIN-Änderung erlaubt nach mindestens (Tage)	Legt den Zeitraum fest, in dem eine PIN nicht erneut geändert werden darf. Diese Einstellung verhindert, dass ein Benutzer seine PIN innerhalb eines bestimmten Zeitraums beliebig oft ändern kann. **Beispiel:** Die Benutzerin Schmidt definiert eine neue PIN (z. B. „13jk56“). Für sie (oder für die Gruppe, der sie zugeordnet ist) ist ein Wechsel nach mind. fünf Tagen festgelegt. Bereits nach zwei Tagen will sie die PIN „13jk56“ ändern. Dies wird abgelehnt, da Frau Schmidt erst nach fünf Tagen eine neue PIN definieren darf.
PIN läuft ab nach (Tage)	Wird die maximale Gültigkeitsdauer aktiviert, muss der Benutzer nach dem eingetragenen Zeitraum seine PIN wechseln und ein neue definieren.

Richtlinieneinstellung	Erklärung
Warnung vor Ablauf (Tage)	Ab “n” Tagen vor Ablauf der PIN wird eine Warnmeldung ausgegeben und der Benutzer darauf hingewiesen, dass er in “n“-Tagen seine PIN ändern muss. Er erhält daraufhin die Möglichkeit, die PIN sofort zu ändern.
ALLGEMEIN	
PIN-Generationen	Bestimmt, wann bereits verwendete PINs wieder verwendet werden dürfen. Sinnvoll ist die Definition von PIN-Generationen insbesondere in Verbindung mit der Einstellung **PIN läuft ab nach** (**Tage**). **Beispiel**: Die Anzahl der PIN-Generationen für den Benutzer Müller wurde auf 4 festgelegt, die der Tage, nach denen der Benutzer die PIN wechseln muss, auf 30. Herr Müller meldete sich bislang mit der PIN „Informatik“ an. Nach Ablauf der Frist von 30 Tagen wird er aufgefordert, seine PIN zu ändern. Herr Müller tippt als neue PIN wieder „Informatik“ ein und erhält die Fehlermeldung, dass er diese PIN bereits verwendet hat und eine andere PIN wählen muss. „Informatik“ darf Herr Müller erst nach der vierten (da PIN-Generationen = 4) Aufforderung zur Eingabe einer neuen PIN verwenden.

15.5 Liste verbotener Kennwörter für die Verwendung mit Richtlinien anlegen

Für Richtlinien des Typs **Kennwort** kann eine Liste mit verbotenen Kennwörtern angelegt werden. Diese Liste definiert die Zeichenfolgen, die in nicht in Kennwörtern verwendet werden dürfen.

Hinweis: In den Listen werden die verbotenen Kennwörter durch einen Leerraum oder einen Zeilenumbruch voneinander getrennt.

TDie Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Textdateien beträgt **50 KB**. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden Sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Konvertierung durchgeführt wird, werden Sie durch eine Meldung darüber informiert.

So registrieren Sie die Textdateien:

1. Klicken Sie im Richtlinien-Navigationsbereich mit der rechten Maustaste auf **Informationstext** und wählen Sie **Neu > Text**.
2. Geben Sie im Feld **Textelementname** einen Namen für den anzuzeigenden Text ein.
3. Wählen Sie über die Schaltfläche **[...]** die zuvor erstellte Textdatei aus. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Informationstext** im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Es wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

15.6 Syntaxregeln für Kennwörter

Kennwörter können sowohl Ziffern, Buchstaben als auch Sonderzeichen (wie + - ; etc.) enthalten. Verwenden Sie bei der Vergabe eines neuen Kennworts jedoch keine Zeichen mit der Kombination ALT + <Zeichen>, da dieser Eingabemodus an der Power-on Authentication nicht zur Verfügung steht. Wie Kennwörter, mit denen sich Benutzer am System anmelden, beschaffen sein müssen, wird in Richtlinien vom Typ **Kennwort** eingestellt.

Achtung: Wenn im SafeGuard Enterprise Management Center Regeln für Kennwörter definiert werden, dann sollten im Active Directory keine Regeln definiert werden.

Richtlinieneinstellung	Erklärung
REGELN	
Mindestlänge des Kennwortes	Zeigt an, aus wie vielen Zeichen ein Kennwort bei der Änderung durch den Benutzer mindestens bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Maximallänge des Kennwortes	Zeigt an, aus wie vielen Zeichen ein Kennwort bei der Änderung durch den Benutzer maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Mindestanzahl an Buchstaben Mindestanzahl an Ziffern Mindestanzahl an Symbolen	Mit diesen Einstellungen wird erreicht, dass Kennwörter nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthalten, sondern aus einer Kombination bestehen müssen (z. B. „15blume“ etc.). Diese Einstellung ist nur dann sinnvoll, wenn eine Kennwortmindestlänge definiert ist, die größer 2 ist.
Groß-/Kleinschreibung beachten	Diese Einstellung wird nur bei den Punkten **Liste nicht erlaubter Kennwörter verwenden** und **Benutzername als Kennwort verboten** wirksam. **Fall 1:** Sie haben in der Liste der verbotenen Kennwörter „Tafel“ eingetragen. Steht die Option **Groß-/Kleinschreibung beachten** auf “JA”, werden zusätzliche Kennwortvarianten wie z. B. „TAFEL“ oder „TaFeL“ nicht akzeptiert und die Anmeldung wird verweigert. **Fall 2:** Der Benutzername für einen Anwender lautet „EMaier“. Steht **Groß-/Kleinschreibung beachten** auf JA und **Benutzername als Kennwort verboten** auf ’NEIN, darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. ´emaier´ oder ´eMaiEr´ etc.) als Kennwort verwenden.

Richtlinieneinstellung	Erklärung
Tastaturzeile verboten	Tastaturzeilen sind „123“ oder „qwe“. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturzeilen beziehen sich nur auf den alphanumerischen Tastaturteil.
Tastaturspalte verboten	Als Tastaturspalten werden eingetippte Zeichenreihen wie „yaq1“, „xsw2“ oder „3edc“ (nicht aber „yse4“, „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als Kennwörter abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Drei oder mehr aufeinanderfolgende Zeichen verboten	Verboten werden mit Aktivierung dieser Option Zeichenketten, ■ die im ASCII-Code aufeinander folgen, sowohl in auf- als auch in absteigender Reihenfolge („abc“; „cba“; „:;<“ etc.). ■ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.
Benutzername als Kennwort verboten	Bestimmt, ob Benutzername und Kennwort identisch sein dürfen. **JA:** Windows-Benutzername und Kennwort müssen unterschiedlich sein. **NEIN**: Benutzer darf seinen Windows-Benutzernamen gleichzeitig als Kennwort verwenden.
Liste nicht erlaubter Kennwörter verwenden	Bestimmt, ob bestimmte Zeichenfolgen für Kennwörter nicht verwendet werden dürfen. Abgelegt sind die Zeichenfolgen in der Liste nicht erlaubter Kennwörter (z. B. Datei im Format .txt).

Richtlinieneinstellung	Erklärung
Liste nicht erlaubter Kennwörter	Definiert Zeichenfolgen, die in einem Kennwort ausgeschlossen sind. Wenn ein Benutzer ein verbotenes Kennwort verwendet, wird eine Fehlermeldung ausgegeben. **Wichtige Voraussetzung:** Eine Liste (eine Datei) mit verbotenen Kennwörtern muss im Management Center unter Informationstext im Richtlinien-Navigationsbereich registriert werden. Erst nach der Registrierung ist die Liste verfügbar. Maximale Dateigröße: 50KB, Unterstütztes Format: Unicode **Nicht erlaubte Kennwörter definieren** In der Liste werden die verbotenen Kennwörter durch einen neuen Zeilenanfang getrennt. *Wildcard*: An der Position, an der Sie den Zeichentyp „*“ eingeben, können mehrere beliebige Zeichen im Kennwort enthalten sein. Beispielsweise wird durch *123* jede Zeichenfolge, die 123 enthält, als Kennwort verboten. **Achtung:** ■ Wenn Sie nur die Wildcard in die Liste einfügen, können sich Benutzer nach einer erzwungenen Kennwortänderung nicht mehr im System anmelden. ■ Benutzer dürfen auf die Datei keinen Zugriff haben. ■ Die Option **Liste nicht erlaubter Kennwörter verwenden** muss aktiviert sein.

Richtlinieneinstellung	Erklärung
Benutzerkennwort-synchronisation mit anderen SGN Clients	Dieses Feld steuert die Synchronisierung bei Änderung des Kennworts durch Benutzer, die auf mehreren SafeGuard Enterprise Benutzer-PCs arbeiten und als Benutzer eingetragen sind. Hier stehen folgende Optionen zur Verfügung: ■ Langsam (sobald Benutzer sich anmeldet) Ändert ein Benutzer sein Kennwort auf einem SafeGuard Enterprise Benutzer-PC, so muss dieser Benutzer sich auf anderen Computern, auf denen er als Benutzer eingetragen ist, zunächst noch einmal mit seinem alten Kennwort an der Power-on Authentication anmelden. Erst dann wird die Kennwortsynchronisation durchgeführt. ■ Schnell (sobald der Computer eine Verbindung hergestellt hat) Ändert der Benutzer sein Kennwort auf einem SafeGuard Enterprise Benutzer-PC, so wird die Kennwortsynchronisierung mit einem anderen Computer, auf dem er als Benutzer eingetragen ist, durchgeführt, sobald der andere Computer eine Verbindung mit dem Server hergestellt hat. Dies erfolgt zum Beispiel dann, wenn sich ein anderer Benutzer, der ebenfalls auf dem Computer als Benutzer eingetragen ist, in der Zwischenzeit an diesem Computer anmeldet.
ÄNDERUNGEN	
Kennwortänderung erlaubt nach mindestens (Tage)	Legt den Zeitraum fest, in dem ein Kennwort nicht erneut geändert werden darf. Diese Einstellung verhindert, dass ein Benutzer sein Kennwort innerhalb eines bestimmten Zeitraums beliebig oft ändern kann. Bei einem durch Windows erzwungenen Kennwortwechsel oder bei einem Wechsel des Kennworts nach der Anzeige der Warnung, dass das Kennwort in x Tagen abläuft, wird diese Einstellung nicht ausgewertet! **Beispiel:** Die Benutzerin Schmidt definiert ein neues Kennwort (z. B. „13jk56“). Für sie (oder für die Gruppe, der sie zugeordnet ist) ist ein Wechsel nach mind. fünf Tagen festgelegt. Bereits nach zwei Tagen will sie das Kennwort „13jk56“ ändern. Dies wird abgelehnt, da Frau Schmidt erst nach fünf Tagen ein neues Kennwort definieren darf.

Richtlinieneinstellung	Erklärung
Kennwort läuft ab nach (Tage)	Wird die maximale Gültigkeitsdauer aktiviert, muss der Benutzer nach dem eingetragenen Zeitraum sein Kennwort wechseln und ein Neues definieren.
Warnung vor Ablauf (Tage)	Ab “n” Tagen vor Ablauf des Kennworts wird eine Warnmeldung ausgegeben und der Benutzer darauf hingewiesen, dass er in “n“-Tagen sein Kennwort ändern muss. Er erhält daraufhin die Möglichkeit, das Kennwort sofort zu ändern.
ALLGEMEIN	
Kennwortgenerationen	Bestimmt, wann bereits verwendete Kennwörter wieder verwendet werden dürfen. Sinnvoll ist die Definition von Kennwortgenerationen insbesondere in Verbindung mit der Einstellung **Kennwort läuft ab nach** (**Tage**). **Beispiel**: Die Anzahl der Kennwortgenerationen für den Benutzer Müller wurde auf 4 festgelegt, die der Tage, nach denen der Benutzer das Kennwort wechseln muss, auf 30. Herr Müller meldete sich bislang mit dem Kennwort „Informatik“ an. Nach Ablauf der Frist von 30 Tagen wird er aufgefordert, sein Kennwort zu ändern. Herr Müller tippt als neues Kennwort wieder „Informatik“ ein und erhält die Fehlermeldung, dass er dieses Kennwort bereits verwendet hat und ein anderes Kennwort wählen muss. „Informatik“ darf Herr Müller erst nach der vierten (da Kennwortgenerationen = 4) Aufforderung zur Eingabe eines neuen Kennworts verwenden.

15.7 Passphrase für SafeGuard Data Exchange

Für den sicheren Datenaustausch über SafeGuard Enterprise Secure Data Exchange muss der Benutzer eine Passphrase eingeben, die für die Erzeugung von lokalen Schlüsseln verwendet wird. Die auf den Endpoint-Computern erzeugten Schlüssel werden auch in der SafeGuard Enterprise Datenbank gespeichert. Welchen Anforderungen diese Passphrase entsprechen muss, wird in Richtlinien vom Typ **Passphrase** eingestellt. Weitere Informationen zu SafeGuard Data Exchange und SafeGuard Portable finden Sie in der SafeGuard Enterprise Benutzerhilfe.

Richtlinieneinstellung	Erklärung
REGELN	
Mindestlänge der Passphrase	Legt fest, aus wie vielen Zeichen die Passphrase, aus der der Schlüssel erzeugt wird, mindestens bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Maximallänge der Passphrase	Legt fest, aus wie vielen Zeichen die Passphrase maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Mindestanzahl an Buchstaben Mindestanzahl an Ziffern Mindestanzahl an Symbolen	Mit diesen Einstellungen wird erreicht, dass eine Passphrase nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthält, sondern aus einer Kombination bestehen muss (z. B. „15blume“ etc.). Diese Einstellung ist nur dann sinnvoll, wenn eine Mindestlänge definiert ist, die größer 2 ist.
Groß-/Kleinschreibung beachten	Diese Einstellung wird beim Setzen der Option „Benutzername als Passphrase verboten“ wirksam. **Beispiel:** Der Benutzername für einen Anwender lautet „EMaier“. Steht **Groß-/Kleinschreibung beachten** auf JA und **Benutzername als Passphrase verboten** auf ’NEIN, darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. ´emaier´ oder ´eMaiEr´ etc.) als Passphrase verwenden.
Tastaturzeile verboten	Tastaturzeilen sind „123“ oder „qwe“. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturzeilen beziehen sich nur auf den alphanumerischen Tastaturteil.

Richtlinieneinstellung	Erklärung
Tastaturspalte verboten	Als Tastaturspalten werden eingetippte Zeichenreihen wie „yaq1“, „xsw2“ oder „3edc“ (nicht aber „yse4“, „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als Passphrase abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Drei oder mehr aufeinanderfolgende Zeichen verboten	Verboten werden mit Aktivierung dieser Option Zeichenketten, ■ die im ASCII-Code aufeinander folgen, sowohl in auf- als auch in absteigender Reihenfolge („abc“; „cba“; „:;<“ etc.). ■ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.
Benutzername als Passphrase verboten	Bestimmt, ob Benutzername und Passphrase identisch sein dürfen. **JA:** Windows-Benutzername und Passphrase müssen unterschiedlich sein. **NEIN**: Benutzer darf seinen Windows-Benutzernamen gleichzeitig als Passphrase verwenden.

15.8 Geräteschutz

Ein Kernstück von SafeGuard Enterprise ist die Verschlüsselung von Daten auf unterschiedlichen Datenträgern. Die Verschlüsselung kann volume- oder dateibasierend durchgeführt werden, mit unterschiedlichen Schlüsseln und Algorithmen. Richtlinien des Typs **Geräteschutz** enthalten auch Einstellungen für SafeGuard Data Exchange und SafeGuard Portable. Weitere Informationen zu SafeGuard Data Exchange und SafeGuard Portable finden Sie in der SafeGuard Enterprise Benutzerhilfe.

Richtlinieneinstellung	Erklärung
Verschlüsselungsmodus für Medien	Dient dem Schutz von Endgeräten (PCs, Notebooks) und allen Arten von Wechseldatenträgern. Hauptaufgabe ist die Verschlüsselung aller auf lokalen oder externen Datenträgern gespeicherten Daten. Durch die transparente Arbeitsweise können Benutzer einfach ihre gewohnten Anwendungen, z. B. Microsoft Office, weiter benutzen. Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (sei es in verschlüsselten Verzeichnissen oder Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie in einem Programm geöffnet werden. Beim Abspeichern der Datei wird diese automatisch wieder verschlüsselt.Folgende Optionen stehen zur Verfügung: ■ **Keine Verschlüsselung** ■ **Volume-basierend** (= **transparente, sektorbasierte Verschlüsselung**) Stellt sicher, dass alle Daten verschlüsselt sind (inkl. Boot-Dateien, Swapfile, Datei für den Ruhezustand/ Hibernation File, temporäre Dateien, Verzeichnisinformationen usw.) ohne dass sich der Benutzer in seiner Arbeitsweise anpassen oder auf Sicherheit achten muss. **Hinweis:** Wenn für ein Volume oder einen Volume-Typ eine Verschlüsselungsrichtlinie existiert und die Verschlüsselung des Volumes schlägt fehl, darf der Benutzer nicht auf das Volume zugreifen.

Richtlinieneinstellung	Erklärung
	Windows 7 System-Partition: Für Windows 7 Professional, Enterprise und Ultimate wird auf dem Endpoint-Computer eine System-Partition angelegt, der kein Laufwerksbuchstabe zugeordnet ist. Diese System-Partition kann nicht von SafeGuard Enterprise verschlüsselt werden.Zugriff auf Unidentified File System Objects: Unidentified File System Objects sind Volumes, die von SafeGuard Enterprise nicht eindeutig als verschlüsselt oder unverschlüsselt identifiziert werden können. Existiert für ein Unidentified File System Volume eine Verschlüsselungsrichtlinie, so wird der Zugriff auf das Volume verweigert. Existiert keine Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen. **Hinweis:** Existiert für ein Unidentified File System Object eine Verschlüsselungsrichtlinie, bei der die Richtlinieneinstellung Schlüssel für die Verschlüsselung auf eine Option eingestellt ist, die die Schlüsselauswahl ermöglicht (z. B. Beliebiger Schlüssel im Schlüsselring des Benutzers), so entsteht zwischen der Anzeige des Schlüsselauswahldialogs und der Verweigerung des Zugriffs auf das Volume eine zeitliche Lücke. Während dieser Zeit kann auf das Volume zugegriffen werden. So lange der Schlüsselauswahldialog nicht vom Benutzer bestätigt wird, besteht Zugriff auf das Volume. Um dies zu vermeiden, definieren Sie einen vorausgewählten Schlüssel für die Verschlüsselung (siehe Beschreibung der Richtlinieneinstellung **Schlüssel für die Verschlüsselung**). Diese zeitliche Lücke entsteht auch dann für mit dem Endpoint-Computer verbundene Unidentified File System Objects, wenn der Benutzer zu dem Zeitpunkt, an dem die Verschlüsselungsrichtlinie wirksam wird, bereits Dateien auf dem Volume geöffnet hat. In diesem Fall, kann nicht gewährleistet werden, dass der Zugriff auf das Volume verweigert wird, da dies zu Datenverlust führen könnte.

Richtlinieneinstellung	Erklärung
	Volumes mit aktivierter Autorun-Funktionalität: Ist für ein Volume, für das eine Verschlüsselungsrichtlinie existiert, die Autorun-Funktionalität aktiviert, so können folgende Probleme auftreten: ■ Das Volume wird nicht verschlüsselt. ■ Wenn es sich um ein UFO handelt, wird der Zugriff nicht verweigert. **Zugriff auf mit BitLocker To Go verschlüsselte Volumes:** Wird SafeGuard Enterprise mit aktivierter BitLocker To Go Unterstützung verwendet und existiert eine SafeGuard Enterprise Verschlüsselungsrichtlinie für ein mit BitLocker To Go verschlüsseltes Volume, so wird der Zugriff auf das Volume verweigert. Existiert keine SafeGuard Enterprise Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen. **Hinweis:** Wenn die Autorun-Einstellungen für ein mit BitLocker To Go verschlüsseltes Volume auf die Standardwerte eingestellt sind, kann es vorkommen, dass der Zugriff trotz vorhandener SafeGuard Enterprise Verschlüsselungsrichtlinie nicht verweigert wird. Diese Situation tritt nur unter Windows Vista auf. Für weitere Informationen zu BitLocker To Go, see *SafeGuard Enterprise und BitLocker To Go* on page 308. ■ Dateibasierend (= transparente, dateibasierte Verschlüsselung (Smart MediaEncryption)) Stellt sicher, dass alle Daten verschlüsselt sind (außer Boot Medium und Verzeichnisinformationen), mit dem Vorteil, dass auch optische Medien wie CD/DVD verschlüsselt werden können oder Daten mit Fremdrechnern, auf denen kein SafeGuard installiert ist, ausgetauscht werden können (soweit von der Richtlinie erlaubt). **Hinweis:** Mit “Dateibasierender Verschlüsselung” verschlüsselte Daten können nicht komprimiert werden. Umgekehrt können auch komprimierte Dateien nicht dateibasierend verschlüsselt werden. Boot-Volumes werden niemals dateibasierend verschlüsselt. Sie sind automatisch von einer dateibasierenden Verschlüsselung ausgenommen, auch wenn eine entsprechende Regel definiert ist.

Richtlinieneinstellung	Erklärung
ALLGEMEINE EINSTELLUNGEN	
Algorithmus für die Verschlüsselung	Setzt den Verschlüsselungsalgorithmus. Liste aller einsetzbaren Algorithmen mit ihren jeweiligen Standards: AES256: 32 Bytes (256 Bits) AES128: 16 Bytes (128 Bits) AES256 mit Diffuser AES128 mit Diffuser
Schlüssel für die Verschlüsselung	Legt fest, welcher Schlüssel zur Verschlüsselung verwendet wird. Es können bestimmte Schlüssel festgelegt werden (z. B. Computer-Schlüssel, oder ein definierter Schlüssel) oder dem Benutzer kann die Auswahl eines Schlüssels erlaubt werden. Die Schlüssel, die ein Benutzer verwenden darf, können eingeschränkt werden. Folgende Optionen stehen zur Verfügung: ■ **Beliebiger Schlüssel im Schlüsselring des Benutzers** Alle Schlüssel aus dem Schlüsselbund des Benutzers werden angezeigt und der Benutzer darf einen daraus auswählen. **Hinweis:** Diese Option muss gewählt werden, wenn eine Richtlinie für dateibasierende Verschlüsselung für einen Standalone Client angelegt wird. ■ **Alle, außer persönliche Schlüssel im Schlüsselring** Alle Schlüssel aus dem Schlüsselbund mit Ausnahme des persönlichen Schlüssels werden angezeigt und der Benutzer darf einen daraus auswählen. ■ **Beliebiger Gruppenschlüssel im Schlüsselring des Benutzers** Alle Gruppenschlüssel aus dem Schlüsselbund des Benutzers werden angezeigt und der Benutzer darf einen daraus auswählen. ■ **Definierter Computer-Schlüssel:** Es wird der Maschinen-Schlüssel verwendet - der Benutzer selbst kann KEINEN Schlüssel auswählen.

Richtlinieneinstellung	Erklärung
	Hinweis: Diese Option muss gewählt werden, wenn eine Richtlinie für volume-basierende Verschlüsselung für einen Standalone Client angelegt wird. Wenn Sie dennoch die Option **Beliebiger Schlüssel im Schlüsselring des Benutzers** auswählen und der Benutzer wählt einen lokal erzeugten Schlüsel für die volume-basierende Verschlüsselung, wird der Zugriff auf dieses Volume verweigert. ■ **Beliebiger Schlüssel im Schlüsselring des Benutzers außer lokal erzeugte Schlüssel** Alle Schlüssel aus dem Schlüsselring mit Ausnahme der lokal erzeugten Schlüsse werden angezeigt und der Benutzer darf einen daraus auswählen ■ **Definierter Schlüssel aus der Liste** Der Administrator kann in der Administration bei der Richtlinien-Einstellung einen beliebigen, existierenden Schlüssel auswählen. **Der Schlüssel muss unter Für Verschlüsselung definierter Schlüssel ausgewählt werden.** **Hinweis:** **Bei Verwendung von „Definierter Computer-Schlüssel“** If SafeGuard Enterprise Device Encryption is not installed on a endpoint computer (no POA, no volume based encryption), a policy defining the **Defined machine key** as the key to be used for file based encryption will not become effective on this computer. The defined machine key is not available on a computer of this type. The data cannot be encrypted. **Richtlinien für durch SafeGuard Enterprise geschützte Standalone-Computer:** Bitte beachten Sie beim Erstellen von Richtlinien für Standalone-Computer, dass für die dateibasierende Verschlüsselung ausschließlich die Option **Beliebiger Schlüssel im Schlüsselring** des Benutzers möglich ist. Zusätzlich darf das Erzeugen von lokalen Schlüsseln nicht verboten werden. Falls die Medien-Passphrase Funktion für Standalone-Computer aktiviert ist, wird der Medienverschlüsselungschlüssel automatisch als **Für Verschlüsselung definierter Schlüssel** verwendet, da auf Standalone Clients keine Gruppenschlüssel zur Verfügung stehen.

Richtlinieneinstellung	Erklärung
	Wenn Sie beim Erstellen einer Wechselmedien-Richtlinie für Standalone-Computer einen anderen Schlüssel unter Für Verschlüsselung definierter Schlüssel auswählen, so hat dies keine Auswirkung.
Für Verschlüsselung definierter Schlüssel	Dieses Feld wird aktiv, wenn Sie im Feld **Schlüssel für die Verschlüsselung** die Option **Definierter Schlüssel aus der Liste** ausgewählt haben. Klicken Sie auf die Schaltfläche **[...]**, um den Dialog **Schlüssel suchen** aufzurufen. Klicken Sie auf **Jetzt suchen**, um nach Schlüsseln zu suchen und wählen Sie einen Schlüssel aus der angezeigten Liste aus. Dies muss in einer Richtlinie vom Typ Geräteschutz mit Ziel des Geräteschutzes: Bei einer Richtlinie vom Typ Geräteschutz mit dem Ziel Wechselmedien wird dieser Schlüssel zur Verschlüsselung des Medienverschlüsselungschlüssel verwendet, wenn die Medien-Passphrase-Funktionalität aktiviert ist (Benutzer darf eine (Medien-)Passphrase definieren : Ja). Für Richtlinien vom Typ Geräteschutz für Wechselmedien müssen daher die Einstellungen ■ Schlüssel für die Verschlüsselung ■ Für Verschlüsselung definierter Schlüssel unabhängig voneinander spezifiziert werden. **Richtlinien für durch SafeGuard Enterprise geschützte Standalone-Computer:** Falls die Medien-Passphrase Funktion für Standalone-Computer aktiviert ist, wird der Medienverschlüsselungschlüssel automatisch als **Für Verschlüsselung definierter Schlüssel** verwendet, da auf Standalone-Computern keine Gruppenschlüssel zur Verfügung stehen.

Richtlinieneinstellung	Erklärung
Benutzer darf einen lokalen Schlüssel erzeugen	Diese Einstellung bestimmt, ob der Benutzer auf seinem Computer lokale Schlüssel erzeugen darf oder nicht. Lokale Schlüssel werden auf dem Endpoint-Computer basierend auf einer vom Benutzer eingegebenen Passphrase erzeugt. Die Anforderungen, denen eine Passphrase entsprechen muss, können in Richtlinien vom Typ **Passphrase** festgelegt werden. Diese Schlüssel werden ebenfalls in der Datenbank gespeichert. Der Benutzer kann sie auf jedem Computer, auf dem er sich anmelden darf, verwenden. Lokale Schlüssel können zum sicheren Datenaustausch über SafeGuard Data Exchange (SG DX) verwendet werden.
VOLUME-BASIERENDE EINSTELLUNGEN	
Benutzer darf dem verschlüsseltem Volume Schlüssel hinzufügen oder diese entfernen	**JA:** Endpoint-Computer-Benutzer darf einen zusätzlichen Schlüssel aus seinem Schlüsselbund einfügen/entfernen. Der Dialog wird angezeigt über den Kontextmenüeintrag **Verschlüsselung /** Registerkarte Verschlüsselung. **NEIN:** Endpoint-Computer-Benutzer darf keinen zusätzlichen Schlüssel einfügen.
Reaktion auf unverschlüsselte Volumes	Definiert, wie Sophos SafeGuard mit unverschlüsselten Medien umgeht: Folgende Optionen stehen zur Verfügung: ■ Abweisen(= Klartext-Medium wird nicht verschlüsselt) ■ Nur unverschlüsselte Medien akzeptieren und verschlüsseln ■ Alle Medien akzeptieren und verschlüsseln
Benutzer darf Volume entschlüsseln	Bewirkt, dass der Benutzer über einen Kontextmenü-Eintrag im Windows Explorer das Laufwerk entschlüsseln darf.
Schnelle Initialverschlüsselung	Wählen Sie diese Einstellung aus, um den Modus der schnellen Initialverschlüsselung für die volume-basierende Verschlüsselung zu aktivieren. Dieser Modus reduziert den Zeitraum, der für die Initialverschlüsselung auf Endpoint-Computern benötigt wird. **Hinweis:** Dieser Modus kann zu einem unsicheren Zustand führen.

Richtlinieneinstellung	Erklärung
Bei defekten Sektoren fortfahren	Legt fest, ob die Verschlüsselung fortgesetzt oder gestoppt werden soll, wenn defekte Sektoren entdeckt werden. Die Standardeinstellung ist JA.
DATEIBASIERENDE EINSTELLUNGEN	
Initialverschlüsselung aller Dateien	Bewirkt, dass die Initialverschlüsselung für ein Laufwerk automatisch nach der Benutzeranmeldung gestartet wird. Der Benutzer muss eventuell vorher einen Schlüssel aus dem Schlüsselbund auswählen.
Benutzer darf Initialverschlüsselung abbrechen	Bewirkt, dass der Benutzer die Initialverschlüsselung abbrechen kann.
Benutzer darf auf unverschlüsselte Dateien zugreifen	Definiert, ob ein Benutzer auf unverschlüsselte Dateien auf einem Laufwerk zugreifen darf.
Benutzer darf Dateien entschlüsseln	Bewirkt, dass der Benutzer einzelne Dateien oder ganze Verzeichnisse entschlüsseln kann (über die Windows Explorer-Erweiterung <rechte Maustaste>).
Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen	Bewirkt, dass der Benutzer eine Medien-Passphrase auf seinem Computer festlegen kann. Die Medien-Passphrase ermöglicht den einfachen Zugriff auf alle lokalen Schlüssel auf Computern ohne SafeGuard Data Exchange über SafeGuard Portable.
Unberücksichtigte Anwendungen	Erlaubt die Definition von Anwendungen, die vom SafeGuard Enterprise Filter-Treiber ignoriert werden sollen und damit von der transparenten Ver-/Entschlüsselung ausgenommen sind. Die einzelnen Anwendungen müssen durch ';' voneinander getrennt werden. Ein Beispiel für eine unberücksichtigte Anwendung kann ein Backup- Programm sein. Damit die Daten beim Erstellen eines Backups nicht entschlüsselt werden, kann diese Anwendung von der Verschlüsselung/Entschlüsselung ausgenommen werden. Die Daten werden verschlüsselt gesichert.

Richtlinieneinstellung	Erklärung
	Hinweis: Da es sich dabei um maschinenspezifische Einstellungen handelt, werden diese erst nach einem Neustart der Benutzer-Computer wirksam.**Unberücksichtigte Anwendungen definieren** Typische Verwendung: Backup-Programme können als unberücksichtigt definiert werden, damit sie immer die verschlüsselten Daten lesen und sichern. Anwendungen, die bei gleichzeitiger Verwendung mit SafeGuard Enterprise Funktionsstörungen auslösen können, aber keine Verschlüsselung brauchen, können generell von der Verschlüsselung ausgenommen werden.Zur Angabe einer unberücksichtigten Anwendung wird der vollständige Name der ausführbaren Datei (optional inklusive Pfadinformation) verwendet. **Hinweis:** Unberücksichtigte Anwendungen können nur global für Lokale Datenträger angegeben werden. Für eine globale Richtlinie vom Typ **Geräteschutz** muss als Ziel **Lokale Datenträger** ausgewählt sein. Für alle anderen Ziele wird diese Option nicht angeboten.
Nur für Wechselmedien SafeGuard Portable auf Wechselmedien kopieren	Ist diese Option eingeschaltet, wird SafeGuard Portable auf jedes Wechselmedium, das mit dem Endpoint-Computer verbunden wird, kopiert. SafeGuard Portable ermöglicht den verschlüsselten Datenaustausch mit wechselbaren Medien, ohne dass der Empfänger der Daten SafeGuard Enterprise installiert haben muss. Der Empfänger kann mit Hilfe von SafeGuard Portable und der entsprechenden Passphrase die verschlüsselten Daten entschlüsseln und auch wieder verschlüsseln. Der Empfänger kann mit SafeGuard Portable die Daten neu verschlüsseln oder den ursprünglich verwendeten Schlüssel für die Verschlüsselung verwenden. SafeGuard Portable muss nicht auf den Computer des Empfängers installiert oder kopiert werden, sondern kann vom wechselbaren Medium verwendet werden.

Richtlinieneinstellung	Erklärung
Standardschlüssel für die Initialverschlüsselung	Über einen Dialog kann ein Schlüssel ausgewählt werden, der für die dateibasierte Initialverschlüsselung verwendet wird. Der Benutzer kann dann beim Start der Initialverschlüsselung keinen Schlüssel wählen. Die Initialverschlüsselung startet ohne Benutzerinteraktion. Für die Initialverschlüsselung wird immer der hier festgelegte Schlüssel verwendet. **Beispiel:** **Voraussetzung:** Ein Standardschlüssel für die Initialverschlüsselung ist gesetzt. Verbindet der Benutzer ein USB-Gerät mit dem Computer, startet die Initialverschlüsselung automatisch. Der definierte Schlüssel wird benutzt. Es ist kein Benutzereingriff notwendig. Will der Benutzer anschließend Dateien umschlüsseln oder neue Dateien auf dem USB-Medium speichern, kann er einen beliebigen Schlüssel auswählen (falls erlaubt und verfügbar). Schließt er dann ein anderes USB-Gerät an, wird wiederum der Schlüssel, der für die Initialverschlüsselung festgelegt wurde, zur Initialverschlüsselung verwendet. Dieser Schlüssel wird auch für folgende Verschlüsselungsoperationen verwendet, bis der Benutzer explizit einen anderen Schlüssel auswählt. **Hinweis:** Wenn die Medien-Passphrase-Funktion aktiviert ist, wird diese Option deaktiviert. Der für die Verschlüsselung definierte Schlüssel wird verwendet.
Klartext-Ordner	Der hier angegebene Ordner wird auf allen Wechselmedien erstellt. Dateien, die in diesen Ordner kopiert werden, bleiben immer unverschlüsselt.

15.9 Spezifische Computereinstellungen - Grundeinstellungen

Richtlinieneinstellung	Erklärung
POWER-ON AUTHENTICATION (POA)	
Power-on Authentication aktivieren	Definiert, ob die POA permanent ein- oder ausgeschaltet sein soll.
Gastbenutzer nicht zulassen	Definiert, ob ein Benutzer zur Windows-Anmeldung zugelassen wird.
Zugriff verweigern, falls keine Verbindung zum Server in Tagen (0 = keine Überprüfung)	Verweigert eine Anmeldung in der POA, wenn der PC länger als festgelegt keine Verbindung mit dem Server hatte.
Nur der zugewiesene Benutzer darf sich anmelden	Definiert, ob ein Benutzer zur Windows-Anmeldung zugelassen wird. **JA:** Lässt nur Benutzer zur Windows-Anmeldung zu, die in der POA bekannt sind. **NEIN:** Lässt Benutzer zur Windows-Anmeldung zu, die in der POA unbekannt sind.
Importieren von neuen Benutzern erlaubt für	Legt fest, ob ein weiterer Benutzer in die POA hinzugefügt werden darf. Hierbei wird unterschieden, ob das nur der Maschineneigentümer (Besitzer) darf oder jeder Benutzer, der bereits in der POA vorhanden ist.

Richtlinieneinstellung	Erklärung
Sicheres Wake On LAN (WOL)	Mit der Richtlinie “Sicheres Wake On LAN“ ist es möglich, den Client für Software-Roll-outs optimal vorzubereiten, indem dafür notwendige Parameter wie das temporäre Deaktivieren der POA und ein Zeitintervall für Wake On LAN dem Client direkt mitgegeben werden können und von ihm ausgewertet werden. Das Roll-out-Team kann durch die zur Verfügung gestellten Kommandos ein Scheduling-Skript so gestalten, dass die größtmögliche Sicherheit des Clients trotz deaktivierter POA gewährleistet bleibt. **Wir weisen an dieser Stelle ausdrücklich darauf hin, dass auch das zeitlich begrenzte "Ausschalten" der POA für eine bestimmte Anzahl von Boot-Vorgängen ein Absenken des Sicherheitsniveaus bedeutet.** **Beispiel:** Das SW-Roll-out Team informiert den SafeGuard Enterprise SO über einen geplanten SW-Roll-out für den 25. September 2010 zwischen 03:00 und 06:00 Uhr. Es sind 2 Neustarts notwendig. Der lokale SW-Roll-out Agent muss sich an Windows anmelden können. Der SO erstellt folgende Richtlinie und weist sie den entsprechenden Endpoint-Computern zu. Anzahl der automatischen Anmeldungen (0 = kein WOL): **5** Anmeldung an Windows erlaubt während WOL: **Ja** Beginn des Zeitfensters für externen WOL Start: **24.Sept. 2010, 12:00** Ende des Zeitfensters für externen WOL Start: **25.Sept. 2010, 06:00** Bei den automatischen Anmeldungen sieht der SO einen Puffer von 3 vor. Das Zeitintervall setzt der SO auf 12:00 Uhr mittags auf den Tag vor dem SW-Roll-out, damit das Scheduling-Skript SGMCMDIntn.exe rechtzeitig starten kann und WOL spätestens am 25.09 um 03:00 Uhr gestartet ist.

Richtlinieneinstellung	Erklärung
	Das SW-Rollout-Team erstellt 2 Kommandos für das Scheduling-Skript: ■ Starte am 24.Sept.2010, 12:15 Uhr SGMCMDIntn.exe / WOLstart ■ Starte am 26.Sept.2010, 09:00 Uhr SGMCMDIntn.exe / WOLstop Das SW-Roll-out-Skript wird auf den 25.09.2010, 03:00 datiert. Am Ende des Skripts kann WOL explizit wieder deaktiviert werden mit SGMCMDIntn.exe /WOLstop. Alle Clients, die sich bis zum 24.Sept.2010 an SafeGuard Enterprise anmelden und mit den Roll-out Servern in Verbindung treten, erhalten die neue Richtlinie und die Scheduling-Kommandos. Jeder Client, auf dem der Scheduler zwischen dem 24. Sept. 2010,12:00 Uhr und dem 25. Sept. 2010, 06:00 Uhr das Kommando SGMCMDIntn /WOLstart auslöst, fällt in das obige WOL-Zeitintervall und aktiviert demzufolge Wake On LAN.
Anzahl der automatischen Anmeldungen	Definiert die Anzahl der Neustarts mit ausgeschalteter Power-on Authentication für Wake On LAN. Diese Einstellung überschreibt temporär die Einstellung von **Power-on Authentication aktivieren**, bis die Anzahl der eingestellten automatischen Anmeldungen erreicht ist. Danach wird die Power-on Authentication wieder aktiviert. Beispiel: Die Zahl der automatischen Anmeldungen ist auf “2” gesetzt, “Power-on Authentication aktivieren” ist eingeschaltet. Der PC bootet zweimal ohne eine Authentisierung in der POA zu verlangen. Wir empfehlen, für Wake On LAN, immer **drei Neustarts mehr als notwendig** zu erlauben, um unvorhergesehene Probleme zu umgehen.
Anmeldung an Windows während WOL erlaubt	Legt fest, ob während eines Wake On LAN ein Logon an Windows erlaubt ist, z. B. für ein SW-Update. Diese Einstellung wird von der POA ausgewertet.

Richtlinieneinstellung	Erklärung
Beginn des Zeitfensters für externen WOL Start Ende des Zeitfensters für externen WOL Start	Datum und Uhrzeit für den Beginn und das Ende des Wake On LAN (WOL) können ausgewählt oder eingegeben werden. Datumsformat: *MM/TT/JJJJ* Zeitformat: *HH:MM* Folgende Eingabekombinationen sind möglich: ■ Beginn und Ende des WOL werden festgelegt. ■ Nur das Ende des WOL wird festgelegt, der Beginn bleibt offen ■ Keine Eingaben: es wird kein Zeitintervall für den Client festgelegt Bei einem geplanten SW-Roll-out sollte der SO den Zeitrahmen für WOL so bemessen, dass das Scheduling-Skript früh genug startet und allen Clients genügend Zeit zum Booten bleibt. WOLstart: Der Startpunkt für den WOL im Scheduling-Skript muss innerhalb des hier in der Richtlinie festgelegten Zeitintervalls liegen. Wenn kein Intervall definiert ist, wird WOL lokal am SafeGuard Enterprise Client nicht aktiviert. WOLstop: Dieses Kommando wird unabhängig vom hier festgelegten Endpunkt des WOL ausgeführt. **Hinweis:** Ab der Version 5.20 wird eine WOL-Einstellung nur wirksam, wenn ein Zeitintervall definiert ist. Das bedeutet im Falle eines Versionsupdates auch, dass mit der Version 5.10 festgelegte WOL-Richtlinien zunächst nicht mehr wirksam sind. Der Sicherheitsbeauftragte muss nach der Migration zusätzlich ein Zeitfenster für diese Richtlinien definieren.
ANZEIGEOPTIONEN	
Computer-Identifikation anzeigen	Zeigt in der Titelleiste der POA entweder den Computernamen oder einen frei definierbaren Text an. Existiert ein Maschinenname in den Windows-Netzwerkeinstellungen, wird dieser in der Grundeinstellung automatisch übernommen.
Text für die Computer-Identifikation	Der Text, der in der Titelleiste der POA angezeigt werden soll. Ist im Feld **Computer-Identifikation anzeigen** die Option **Definierter Name** ausgewählt, können Sie in diesem Eingabefeld den Text eingeben.

Richtlinieneinstellung	Erklärung
Rechtliche Hinweise anzeigen	Zeigt eine Textbox mit frei konfigurierbarem Inhalt an, die vor der Anmeldung in der POA erscheint. In manchen Ländern ist das Erscheinen eines Textfelds mit bestimmtem Inhalt gesetzlich vorgeschrieben. Die Box muss vom Benutzer bestätigt werden, bevor das System fortfährt. Bevor Sie einen Text angeben können, muss dieser als Textelement im **Richtlinien-Navigationsbereich** unter **Informationstext** registriert werden
Text für rechtliche Hinweise	Text, der als rechtlicher Hinweis angezeigt werden soll. Sie können hier ein Textelement auswählen, das im **Richtlinien-Navigationsbereich** unter **Informationstext** registriert wurde.
Zusätzliche Informationen anzeigen	Zeigt eine Textbox mit frei konfigurierbarem Inhalt an, die nach den rechtlichen Hinweisen (wenn diese aktiviert sind) erscheint. Sie können festlegen, ob die zusätzlichen Informationen ■ Nie ■ Bei jedem Systemstart ■ Bei jeder Anmeldung angezeigt werden.
Text für zusätzliche Informationen	Text, der als zusätzliche Information angezeigt werden soll. Sie können hier ein Textelement auswählen, das im **Richtlinien-Navigationsbereich** unter **Informationstext** registriert wurde.
Anzeigedauer (in Sekunden)	Zeitraum (in Sekunden) für die Anzeige zusätzlicher Informationen. Sie können hier die Anzahl der Sekunden eingeben, nach denen die Textbox für zusätzliche Informationen automatisch geschlossen wird. Der Benutzer kann die Textbox jederzeit durch Klicken auf **OK** schließen.

Richtlinieneinstellung	Erklärung
System Tray Icon aktivieren und anzeigen	Über das SafeGuard Enterprise System Tray Icon kann auf dem Endpoint-Computer einfach und schnell auf alle Benutzerfunktionen zugegriffen werden. Zusätzlich können für den Benutzer Informationen über den Status des Computers (neue Richtlinien erhalten, ...) über Balloon Tool Tips ausgegeben werden **Ja:** System Tray Icon wird im Infobereich der Taskleiste angezeigt, der Benutzer wird über Balloon Tool Tips laufend über den Status des durch SafeGuard Enterprise geschützten Computer. **Nein:** System Tray Icon wird nicht angezeigt. Keine Statusinformationen für den Benutzer über Ballon Tool Tips. **Stumm:** System Tray Icon wird im Infobereich der Taskleiste angezeigt, es werden aber keine Statusinformationen für den Benutzer über Ballon Tool Tips ausgegeben.
Overlay-Symbole im Explorer anzeigen	Bestimmt, ob im Windows Explorer Schlüsselsymbole zur Anzeige des Verschlüsselungsstatus von Volumes, Geräten, Ordnern und Dateien angezeigt werden.
Virtuelle Tastatur in der POA	Bestimmt, ob im POA-Anmeldedialog bei Bedarf eine virtuelle Tastatur zur Eingabe des Kennworts angezeigt werden kann.
INSTALLATIONSOPTIONEN	
Deinstallation erlaubt	Bestimmt, ob die Deinstallation von SafeGuard Enterprise auf den Client-Computern möglich ist. Wird **Deinstallation erlaubt** auf ***Nein*** gesetzt, kann SafeGuard Enterprise solange eine Richtlinie mit dieser Einstellung wirksam ist, auch mit Administratorrechten nicht deinstalliert werden.
EINSTELLUNGEN FÜR DIE KRYPTOGRAPHISCHE BASISINFRASTRUKTUR	
Windows Cryptographic Toolkits	Mögliche Optionen: ■ SafeGuard Cryptographic Engine ■ AET SafeSign TPM Unterstützung Hardwarezufallszahlengenerator; Benötigt ein spezielles Mainboard im PC.

Richtlinieneinstellung	Erklärung
TOKENUNTERSTÜTZUNG: EINSTELLUNGEN FÜR PKCS #11 MODUL 1	
Modulname	Registriert das PKCS#11 Modul eines Token. Zur Auswahl stehen: ■ Siemens CardOS API ■ AET SafeSign Identity Client ■ Charismatics Smart Security Interface ■ Aladdin eToken PKI Client ■ RSA Authentication Client 2.x ■ RSA Smart Card Middleware 3.x ■ ActivIdentity ActivClient ■ a.sign Client ■ Gemalto .NET Card ■ Gemalto Classic Client ■ Gemalto Access Client ■ IT Solution trustWare CSP+ ■ Estonian ID Card ■ NetKey 3.0

Richtlinieneinstellung	Erklärung
	Lizenzinformationen für Siemens und Charismatics: Beachten Sie, dass für die Benutzung der jeweiligen Middleware für das Standard-Betriebssystem eine Lizenzvereinbarung mit Siemens Medical/Charismatics erforderlich ist. Um Lizenzen zu erwerben, wenden Sie sich bitte an: ■ Global Siemens Healthcare Headquarters Siemens AG Healthcare Sector Henkestrasse 127 D-91052 Erlangen Tel.: +49 69 797 6602 ■ *http://www.charismathics.com/cryptoshop/shop_content.php* oder sales@charismathics.com
Dienste, auf die gewartet wird	Diese Einstellung dient zur Problembehebung mit bestimmten Token. Entsprechende Einstellungen werden gegebenenfalls von unserem Support bekanntgegeben.

16 SafeGuard Configuration Protection

Netzwerke in Unternehmen sind heute durch eine Vielzahl an leicht zugänglichen Ports, z. B. USB, FireWire und PCMCIA, gekennzeichnet. Darüber hinaus ermöglicht eine Reihe verschiedener Datenanschlussgeräte (z. B. Bluetooth, IrDA und WLAN) sowie Gerätetypen (z. B. externe Speichergeräte, Drucker, Digitalkameras, Smartphones und PDAs) den einfachen Zugang zu Endpoints. die diese Ports und Geräte nutzen.

Diese Geräte ermöglichen optimale Zugänglichkeit und Produktivität. Die Endpoints sind dadurch jedoch offen und es besteht die Gefahr der Infiltration. Schätzungen zufolge befinden sich über 60 % der Daten eines Unternehmens auf Endpoints. Somit bilden sie den wertvollsten und zugleich verwundbarsten Teil eines Unternehmensnetzwerks.

Im IT-Bereich eines Unternehmens werden häufig Kompromisse zwischen Produktivität und Sicherheit eingegangen. Aufgrund der hohen Produktivitätsanforderungen sind innovative Geräte und Sicherheitskonzepte für Unternehmen sehr interessant. Die Umsetzung von äußerst effektiven und verlässlichen Sicherheitsmaßnahmen gegen Informationslecks, Diebstahl, Betrug, Viren, Abhören und Missbrauch von Informationen und Ressourcen stellt Unternehmen jedoch vor große Herausforderungen.

Untersuchungen haben ergeben, dass 70 % aller Sicherheitsrisiken und Sicherheitsverletzungen innerhalb des Unternehmens selbst auftreten. Die höchste Priorität von Unternehmen ist daher die interne Sicherheit, vor allem der interne Zugang zu Netzwerkressourcen, noch vor Gateway-Lösungen wie Antivirenprogramme und Firewalls. Die größte Herausforderung, was die Sicherheit im Unternehmen angeht, besteht darin, den Zugang zu wichtigen Unternehmensdaten zu ermöglichen, ohne diese zu gefährden. Darüber hinaus soll internen Benutzern Vertrauen entgegengebracht werden, gleichzeitig soll jedoch die Möglichkeit bestehen, ihre Verlässlichkeit zu prüfen.

Echter Schutz lässt sich nur durch Errichten einer „digitalen Mauer“ um jeden einzelnen Computer erreichen: die einzelnen Ports müssen intelligent geschützt, der Zugang zu zugelassenen Geräten muss überlegt gewährt werden.

16.1 Die SafeGuard Configuration Protection Lösung

In Verbindung mit SafeGuard PortAuditor (siehe *SafeGuard PortAuditor User Guide*) bietet SafeGuard Configuration Protection eine umfassende Lösung. Mit dieser Lösung erhalten Unternehmen einen Überblick darüber, welche Ports und Geräte innerhalb des Unternehmens benutzt werden (**Sichtbarkeit**). Darüber hinaus können sie eine Richtlinie definieren, die die Benutzung **kontrolliert** und die Daten beim Übertragen **schützt**.

SafeGuard Configuration Protection kontrolliert jeden Endpoint und jedes Gerät über jedes Netzwerk an allen Schnittstellen. Das Modul überwacht den Datenverkehr in Echtzeit und wendet darauf abgestimmte, detailliert einstellbare Sicherheitsrichtlinien für alle Arten von Schnittstellen und externen Speichergeräten an:

1. **Physikalische Ports:**
   a) USB
   b) FireWire
   c) PCMCIA
   d) Secure Digital (SD)
   e) Parallel
   f) Seriell
   g) Modem
2. **Wireless Ports:**
   a) WLAN
   b) Bluetooth
   c) Infrarot (IrDA)
3. **Externe Speicher:**
   a) Wechselmedien
   b) Externe Festplatten
   c) CD/DVD-Laufwerke
   d) Diskettenlaufwerke
   e) Magnetbandlaufwerke

SafeGuard Configuration Protection erkennt Gerätetypen, Modelle und sogar spezifische Seriennummern und ermöglicht eine Einschränkung der Benutzung nach diesen Angaben. Mit SafeGuard Configuration Protection können Sicherheitsbeauftragte alle Speichermedien vollständig blockieren. WLAN-Kontrollen basieren auf MAC-Adresse, SSID oder Netzwerksicherheitsebene.

16.1.1 Funktionen

1. **Port-Kontrolle**
   Mit SafeGuard Configuration Protection können Sie die Benutzung bestimmter oder aller Computer-Ports innerhalb Ihres Unternehmens nach dem jeweiligen Computer, dem angemeldeten Benutzer und/oder dem Port-Typ zulassen, sperren oder einschränken. SafeGuard Configuration Protection kontrolliert USB, PCMCIA, FireWire, Secure Digital, Serial, Parallel, Modem (z. B. Dial-Up, 3G usw.), WLAN, IrDA und Bluetooth Ports.

2. **Gerätekontrolle**
   SafeGuard Configuration Protection bietet die detailliert einstellbare Identifikation und Zulassung von Geräten mit einer umfassenden Liste von Gerätetypen und durch Erstellung von White Lists mit Gerätetypen oder einzelnen Geräten (nach Seriennummer).

3. **Speicherkontrolle**
   SafeGuard Configuration Protection bietet spezielle Kontrolle externer und interner Speichergeräte, u. a. Wechselmedien, externe Festplatten, CD/DVD, Diskette und Band. Über eine Richtlinie lassen sich Gerätetypen, Modelle und einzelne Geräte (nach Seriennummer) sperren.

4. **Hybrid Network Bridging blockieren**
   Mit SafeGuard Configuration Protection können Sicherheitsbeauftragte die gleichzeitige Nutzung verschiedener Netzwerkprotokolle, die zu unabsichtlichem oder absichtlichem Hybrid Network Bridging (z. B. WLAN Bridging und 3G Card Bridging) führen kann, kontrollieren und verhindern. SafeGuard Configuration Protection Clients lassen sich so konfigurieren, dass der Zugang zu WLAN, Bluetooth, Modems oder IrDA-Links gesperrt ist, wenn die Haupt-TCP/IP-Netzwerkschnittstelle mit dem Netzwerk verbunden ist. Benutzer können somit die verschiedenen Netzwerkprotokolle nur dann anwenden, wenn sie keine Verbindung zum Netzwerk haben. Dadurch lassen sich Erzeugung und möglicher Missbrauch einer Hybrid Network Bridge vermeiden.

Hinweis: Interne Ports, z. B. Speicher-BUS wie IDE, SCSI, ATA und S-ATA, die zum Anschließen interner Festplattenlaufwerke sowie PCI und PCI-X verwendet werden, sind standardmäßig zugelassen.

5. **USB und PS/2 Hardware Key Logger blockieren**
   Mit SafeGuard Configuration Protection lassen sich USB Hardware Key Logger, die jeden Tastendruck auf den Endgeräten verfolgen und aufzeichnen, sperren und PS/2 Hardware Key Logger unbrauchbar machen.

6. **Benachrichtigungen für Benutzer**
   Wenn SafeGuard Configuration Protection eine Richtlinie auf einem Client wirksam werden lässt, wird der Benutzer durch eine Meldung über gesperrte Ports und Geräte benachrichtigt.

16.2 Schutz durch SafeGuard Configuration Protection

SafeGuard Configuration Protection schützt Ihre Endpoints wie in den folgenden Abschnitten beschrieben.

16.2.1 Port-Kontrolle

Mit SafeGuard Configuration Protection können Sie die Benutzung bestimmter oder aller Computer-Ports innerhalb Ihres Unternehmens nach dem jeweiligen Computer, dem angemeldeten Benutzer und/oder dem Port-Typ zulassen, sperren oder einschränken. SafeGuard Configuration Protection kontrolliert USB, PCMCIA, FireWire, Secure Digital, Serial, Parallel, Modem (z. B. Dial-Up, 3G usw.), WLAN, IrDA und Bluetooth Ports.

Ein gesperrter Port steht nicht zur Verfügung. Wenn der Computer startet, oder eine Richtlinie angewendet wird, die einen zuvor zugelassenen Port blockiert, wird eine entsprechende Meldung angezeigt.

16.2.2 Gerätekontrolle

Neben der Kontrolle von Portzugängen, bietet SafeGuard Configuration Protection eine weitere Detailebene. Mit SafeGuard Configuration Protection können Sie festlegen, welche Geräte auf einen Port zugreifen dürfen.

Für USB, PCMCIA und FireWire Ports können Sie festlegen, welche Gerätetypen, Gerätemodelle und/oder Einzelgeräte auf einen Port zugreifen können:

- **Gerätetypen:**
  Mit dieser Option können Sie den Zugriff auf einen Port nach dem Typ des Geräts, das an dem Port angeschlossen ist, einschränken. Bei Gerätetypen handelt es sich zum Beispiel um Drucker, Netzwerkadapter, Eingabegeräte (z. B. Maus) oder Audio/Video-Geräte.
  Die auswählbaren Gerätetypen sind in SafeGuard Configuration Protection integriert. Wenn Sie ein Gerät zulassen möchten, das nicht in der Typenliste aufgeführt ist, können Sie die Optionen **White List für Gerätemodelle** oder **White List für einzelne Geräte** wie nachfolgend beschrieben verwenden.

- **White List für Gerätemodelle:**
  Diese Option bezieht sich auf das Modell eines bestimmten Gerätetyps, z. B. alle HP-Drucker oder alle USB-Sticks des Modells M-Systems.

- **White List für einzelne Geräte:**
  Diese Option bezieht sich auf eine Liste einzelner Geräte mit jeweils eindeutiger Seriennummer (einzelne spezifische Geräte). Zum Beispiel: der PDA des CEO ist zugelassen, alle anderen PDAs sind gesperrt.

Schutz gegen Hardware Key Logger

Hardware Key Logger sind Geräte, die in bösartiger Absicht zwischen Tastatur und Computer angebracht werden, um die Tastatureingaben nachzuverfolgen und aufzuzeichnen und sich somit wertvolle Informationen, insbesondere ID und Kennwort, anzueignen.

Mit SafeGuard Configuration Protection können Sie die Anwender vor dieser Bedrohung schützen: SafeGuard Configuration Protection erkennt Hardware Key Logger, die an einen USB- oder PS/2-Port angeschlossen sind. In einer Richtlinie können Sie festlegen, ob Hardware Key Logger bei ihrer Entdeckung blockiert werden sollen.

16.2.3 Speicherkontrolle

Die Speicherkontrolle bietet eine zusätzliche Detailebene bei der Festlegung der Sicherheitsanforderungen im Unternehmen. Die Speicherkontrolle kann sich auf alle Speichergeräte beziehen: interne oder externe Speicher - fest angebrachte oder abnehmbare Speichergeräte.
Sie können Speichergeräte vollständig sperren.

Ähnlich wie die im vorigen Abschnitt beschriebenen Nicht-Speichergeräte können auch Speichergeräte nach Typ, Modell oder Einzelkennung zugelassen werden.

Autorun Kontrolle

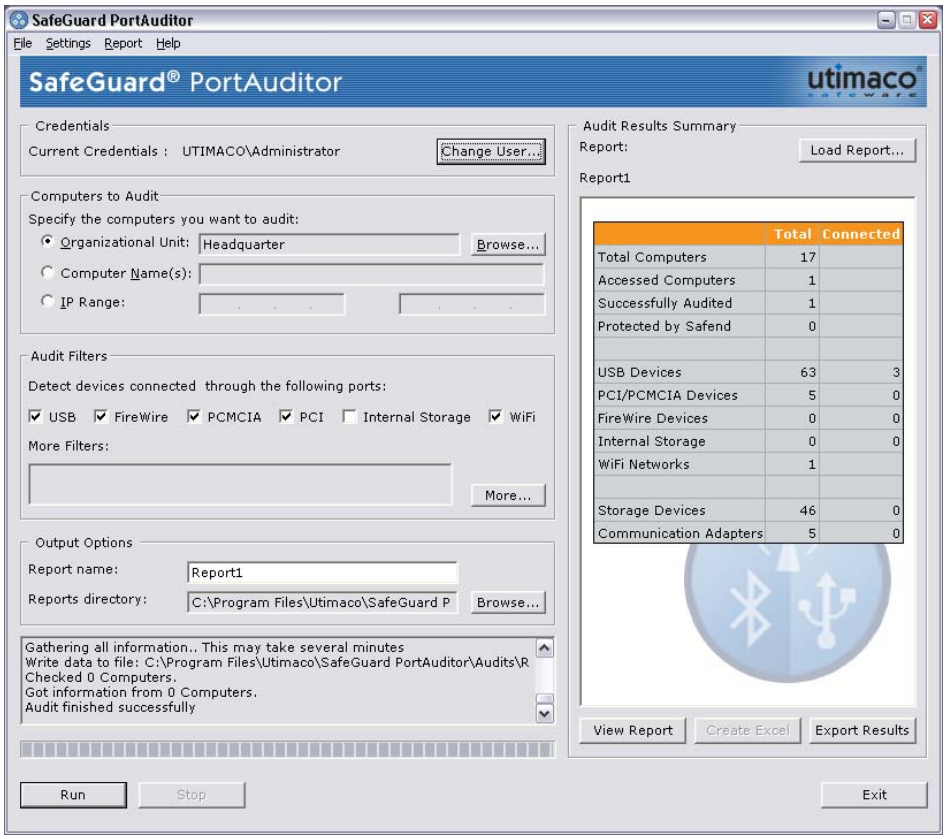
Mit SafeGuard Configuration Protection können Sie die Verwendung von neuen hoch entwickelten Speichergeräten durch die Endbenutzer zulassen und dabei sicherstellen, dass die Endgeräte vor Sicherheitsrisiken durch Anwendungen, die die Geräte bieten, geschützt sind. Im Rahmen der Sicherheitsrichtlinie können Sie Autostart-Vorgänge blockieren. Unter Anwendung unserer einzigartigen granularen Client-Technologie können Sie Smart-Speichergeräte zulassen, wenn diese Ihrer Speicherrichtlinie entsprechen, und nur die potenziell unsichere Autorun-Funktionalität blockieren.

16.2.4 WLAN-Kontrolle

Die WLAN-Kontrolle stellt sicher, dass Benutzer nur die zugelassenen Netzwerke benutzen. Sie können festlegen, welche Netzwerke oder Ad-hoc-Links Zugang erhalten. Die zugelassenen Verbindungen lassen sich durch Angeben der MAC-Adresse der Zugangspunkte, der SSID des Netzwerks, der Authentisierungsmethode und der Verschlüsselungsmethoden definieren.

16.2.5 SafeGuard PortAuditor

Mit SafeGuard PortAuditor steht Ihnen zusätzlich zu SafeGuard Configuration Protection ein umfangreiches Werkzeug zur Verfügung. Der SafeGuard PortAuditor bietet in Ergänzung zu SafeGuard Configuration Protection einen vollständigen Überblick darüber, welche Ports, Geräte und Netzwerke von den Benutzern im Unternehmen benutzt werden (oder wurden). Das Ergebnis einer SafeGuard PortAuditor Abfrage können Sie zur Auswahl der Geräte und Netzwerke, die Sie zulassen möchten, benutzen.



Weitere Informationen hierzu finden Sie im *SafeGuard PortAuditor User Guide*.

16.3 Richtlinien für den Konfigurationsschutz

In einer Richtlinie vom Typ **Konfigurationsschutz** wird festgelegt, welche Ports zugelassen, gesperrt oder eingeschränkt sind. Werden Ports **eingeschränkt**, so bedeutet dies, dass nur die angegebenen Gerätetypen, Gerätemodelle, Einzelgeräte oder WLAN-Verbindungen Zugang über den betreffenden Port erhalten sollen.

Eine Richtlinie definiert auch die Zugangsberechtigungen von Speichergerättypen, Speichergerätmodellen oder einzelnen Speichergeräten sowie WLAN-Verbindungen. Hier können Sie (entsprechend der Vorgehensweise für Geräte) festlegen, ob Speichergeräte zugelassen, gesperrt oder eingeschränkt werden sollen.

Über eine Richtlinie lassen sich auch **Hardware Key Logger**, die an einen USB- oder PS/2-Port angeschlossen werden, blockieren. Hardware Key Logger sind Geräte, die in bösartiger Absicht zwischen der Tastatur und dem Computer angebracht werden, um die Tastatureingaben zu protokollieren. In Ihrer Richtlinie können Sie festlegen, ob Hardware Key Logger blockiert werden sollen, wenn sie durch SafeGuard Configuration Protection erkannt werden.

SafeGuard Configuration Protection lässt standardmäßig alle Geräte zu, es sei denn, Sie definieren eine Richtlinie, die den Zugang blockiert.

Die folgenden Abschnitte beschreiben die Vorgehensweise beim Anlegen einer Richtlinie.

16.3.1 Richtlinien für den Konfigurationsschutz definieren - Workflow

Der folgenden Abschnitte bieten einen Überblick zum Workflow für das Definieren einer neuen Richtlinie. Jeder einzelne Schritt verweist auf den jeweiligen Unterabschnitt, der den Schritt im Detail beschreibt.

Der Workflow schlägt eine einfache und direkte Vorgehensweise für die Durchführung der einzelnen Schritte vor. Nach Wunsch können Sie von der vorgeschlagenen Reihenfolge abweichen.

- ***Schritt 1: Computer scannen und Port-/Geräte-/WLAN-Nutzung ermitteln***:
  Scannen Sie mit SafeGuard PortAuditor die Computer in Ihrem Netzwerk, um die Geräte und WLAN-Netzwerke zu ermitteln, die derzeit angeschlossen sind und zu früheren Zeitpunkten angeschlossen waren (in der Registry des Computers angegeben). Gehen Sie hierzu wie im *SafeGuard PortAuditor User Guide* beschrieben vor. Mit diesen Informationen können Sie beim Definieren einer Richtlinie auf einfache Art und Weise die Ports und Geräte angeben, die zugelassen, blockiert oder eingeschränkt werden sollen.
- ***Schritt 2: Richtlinie planen***
  Beschreibt das Sammeln der notwendigen Informationen für die Planung der optimalen Schutzrichtlinie für Ihr Unternehmen.

- ***Schritt 3: Richtlinie erstellen***
  Beschreibt das Erstellen einer neuen Richtlinie. Sie können je nach Ihren Anforderungen beliebig viele Richtlinien - eine Richtlinie für das gesamte Unternehmen oder unterschiedliche Richtlinien für die einzelnen Computer- oder Benutzergruppen - erstellen.

- ***Schritt 4: Portkontrolle definieren***
  Beschreibt die Definition der Portkontrolle in Ihrer Richtlinie. Hier legen Sie fest, welche Ports zugelassen sind, welche gesperrt sind und welche nur von bestimmten Geräten benutzt werden dürfen. Darüber hinaus beschreibt dieser Abschnitt, wie Sie Hybrid Network Bridging vermeiden.

- ***Schritt 5: Gerätekontrolle definieren***
  Beschreibt, wie Sie die Geräte, die über die eingeschränkten Ports auf Ihren Endgeräten angeschlossen werden dürfen, festlegen.

- ***Schritt 6: Speicherkontrolle definieren***
  Beschreibt, wie Sie die Speichergeräte, die über die eingeschränkten Ports auf Ihren Endgeräten angeschlossen werden dürfen, festlegen.

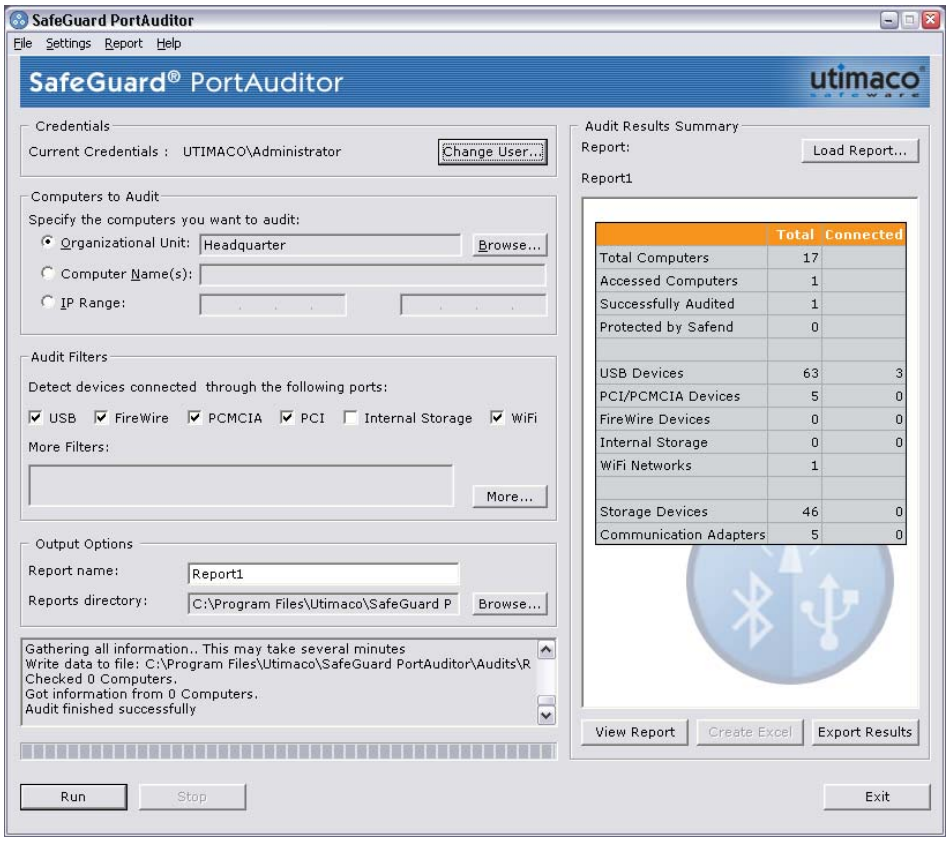
- ***Schritt 7: WLAN-Kontrolle definieren***
  Beschreibt die Definition der zugelassenen WLAN-Verbindungen.

- ***Schritt 8: Dateikontrolle definieren***
  Beschreibt, wie Sie die Berechtigungen für Dateitypen, die von und an Speichergeräte übertragen werden, festlegen.

- ***Schritt 9: Richtlinie speichern und veröffentlichen***
  Beschreibt die Optionen für das Speichern der Richtlinie in der Richtliniendatenbank sowie für das Veröffentlichen der Richtlinie, um sie den betreffenden Clients zuzuweisen.

16.3.2 Schritt 1: Computer scannen und Port-/Geräte-/WLAN-Nutzung ermitteln

Mit SafeGuard PortAuditor steht Ihnen zusätzlich zu SafeGuard Configuration Protection ein umfangreiches Werkzeug zur Verfügung. Der SafeGuard PortAuditor bietet in Ergänzung zu SafeGuard Configuration Protection einen vollständigen Überblick darüber, welche Ports, Geräte und Netzwerke von den Benutzern im Unternehmen benutzt werden (oder wurden). Das Ergebnis einer SafeGuard PortAuditor Abfrage können Sie zur Auswahl der Geräte und Netzwerke, die Sie zulassen möchten, benutzen.



16.3.3 Schritt 2: Richtlinie planen

Bevor Sie mit der Definition der Richtlinie beginnen, sollten Sie die für Ihr Unternehmen optimal geeignete Richtlinie entwerfen. Die optimale SafeGuard Configuration Protection Richtlinie für Ihr Unternehmen erfüllt Ihre Sicherheitsanforderungen und entspricht gleichzeitig den Anforderungen der Personen, die Zugang zu den Computern im Unternehmen über die Ports benötigen.

Im ersten Schritt sollte festgelegt werden, für welche Arten von Organisationseinheiten (Organizational Units, OUs) und Gruppen die Richtlinien gelten sollen.

Benutzer- und Computerrichtlinien

SafeGuard Configuration Protection verwendet standardmäßig Benutzergruppen- und Computergruppendefinitionen, die durch Active Directory gesteuert werden. Jede Option bietet eigene Vorteile:

- **Nach Benutzergruppen:**
  Wenn Sie Ihre Richtlinien nach Benutzergruppen definieren, können Sie die spezifischen Berechtigungen für jeden Benutzer festlegen.
  Richtlinien, die für Benutzer gelten, haben Priorität gegebenüber Richtlinien, die für Computer gelten.
  Wenn Sie sich dafür entscheiden, Richtlinien Benutzergruppen zuzuweisen, empfehlen wir, trotzdem eine oder mehrere allgemeine Richtlinien für Computer zu erstellen. Auf diese Weise lässt sich jeder einzelne Computer-Port auch dann schützen, wenn kein Benutzer angemeldet ist.
  Wenn Sie Benutzerrichtlinien und Maschinenrichtlinien in Kombination verwenden, können Sie z. B. alle USB-Speichergeräte auf allen Computern in der Abteilung Kundenservice blockieren und gleichzeitig dem Abteilungsleiter eine liberalere Richtlinie nach Benutzername und Kennwort zuordnen, bei der es keine Rolle spielt, auf welchem Computer die Anmeldung erfolgt.

- **Nach Computergruppen:**
  Wenn Sie Ihre Richtlinien nach Computern definieren, können Sie die Endgeräte im Unternehmen schützen, ohne dass es eine Rolle spielt, welcher Benutzer angemeldet ist.

SafeGuard Configuration Protection setzt die Richtlinien wie folgt in Kraft:
Zuerst wird eine Benutzerrichtlinie angewendet, wenn eine Richtlinie für den derzeit angemeldeten Benutzer vorhanden ist. Ist dies nicht der Fall, sucht SafeGuard Configuration Protection nach einer Richtlinie, die für den Computer gilt, und wendet diese an (falls vorhanden). Ist also kein Benutzer angemeldet, so wird die computergebundene Richtlinie angewendet. Daher ist es empfehlenswert, benutzerbasierte Richtlinien zu verteilen, so dass jeder Benutzer unabhängig vom Computer, auf dem er sich anmeldet, dieselbe Richtlinie erhält, und restriktivere computerbasierende Richtlinien zu definieren. Die computerbasierenden Richtlinien sollten auch dann die Benutzung von Geräten wie Maus und Tastatur zulassen, wenn kein Benutzer oder ein Benutzer außerhalb der Domäne angemeldet ist.

Die initiale Konfiguration des SafeGuard Protection Client lässt Port- und Geräteaktivitäten vollständig zu, d. h. nichts ist blockiert. Dies ist notwendig, damit nicht alle Port-Aktivitäten automatisch nach der Installation des SafeGuard Configuration Protection Client blockiert werden.

Ein Computer, auf dem SafeGuard Configuration Client gerade installiert wurde, arbeitet somit wie zuvor (Ports und Geräte sind nicht blockiert), bis Sie Richtlinien definieren und an Ihre Endgeräte (nach Benutzer oder Computer) verteilen.

Hinweis: Die Maschinenrichtlinie wird als Ersatzrichtlinie verwendet, falls die Benutzerrichtlinie nicht verwendet werden kann oder beschädigt ist. Es ist daher empfehlenswert, sowohl eine Maschinen- als auch eine Benutzerrichtlinie zu erstellen, wobei die Benutzerrichtlinie nicht so restriktiv wie die Maschinenrichtlinie sein sollte.

Hinweis: Je nach Benutzercomputer kann es einige Sekunden dauern, bis auf dem SafeGuard Configuration Protection Client nach der Anmeldung eine Richtlinienänderung wirksam wird. Wenn die Maschinenrichtlinie restriktiver ist als die Benutzerrichtlinie, kann es somit einige Sekunden dauern, bis der Zugriff auf die Geräte für den Benutzer gewährt wird.

16.3.4 Schritt 3: Richtlinie erstellen

Die Erstellung von Richtlinien vom Typ Konfigurationsschutz erfolgt wie für alle anderen Richtlinien beschrieben.

16.3.5 Schritt 4: Port-Kontrolle definieren

Dieser Schritt umfasst sowohl die Definition von Zulassungseinstellungen für Ports als auch für Hybrid Network Bridging.

Zulassungseinstellungen für Ports

SafeGuard Configuration Protection ermöglicht positiven Schutz durch Zulassen des Zugangs zu allen Ports auf allen Computern, an die eine Richtlinie verteilt wird, es sei denn, die Richtlinie gibt an, dass der Zugang zu einem betreffenden Port gesperrt ist (siehe folgende Absätze).

Für jeden Port (USB, FireWire, PCMCIA, Secure Digital, Seriell, Parallel, Modem, WLAN, IrDA, oder Bluetooth) können Sie aus folgenden Optionen wählen:

- **Zulassen:**
  Diese Option gibt an, dass der Port beliebig ohne Einschränkungen auf diesem Kommunikationskanal genutzt werden darf.

- **Sperren:**
  Diese Option legt fest, dass über den betreffenden Port kein Zugang besteht. Der Port steht nicht zur Verfügung.

- **Einschränken:**
  Für USB-, FireWire-, PCMCIA- und WLAN-Ports können Sie auch festlegen, dass der Zugang zu Ports dieser Art eingeschränkt werden soll. Bei Auswahl der Option **Einschränken** können Sie die Geräte oder Verbindungen, die auf den Port zugreifen dürfen, genauer (d. h. mit höherer Granularität) definieren. So können Sie zum Beispiel festlegen, dass nur USB-Geräte eines bestimmten Modells oder nur spezifische USB-Geräte (d. h. Einzelgeräte mit eindeutiger Seriennummer) zugelassen sind. Für physikalische Ports erfolgt dies über die Option *Gerätekontrolle* (siehe *Schritt 5: Gerätekontrolle definieren*) sowie über die Option *Speicherkontrolle* (siehe *Schritt 6: Speicherkontrolle definieren*). Für Wireless-Ports wird die Option *WLAN-Kontrolle* (siehe *Schritt 7: WLAN-Kontrolle definieren*) benutzt.

Hinweis: Die Bereiche Gerätekontrolle und WLAN-Kontrolle einer Richtlinie gelten nur für Ports, die als eingeschränkt definiert sind. Der Bereich Speicherkontrolle einer Richtlinie gilt sowohl für eingeschränkte als auch für zugelassene Ports.

Legen Sie für jeden Port den gewünschten Aktionstyp (**Zulassen**, **Sperren** oder **Einschränken**) fest, indem Sie die betreffende Option aus der Dropdownliste des jeweiligen Felds auswählen.

Hinweis: Interne Ports, z. B. Speicher-BUS wie IDE, SCSI, ATA and S-ATA, die zum Anschließen interner Festplattenlaufwerke sowie PCI und PCI-X verwendet werden, sind standardmäßig zugelassen.

Hinweis: Die Einstellungen für SecureDigital im Bereich *Physikalische Ports* sind relevant, wenn SecureDigital als Port benutzt wird. Wenn SecureDigital über einen USB-Adapter angeschlossen ist, wird es als USB-Massenspeicher eingestuft. Wenn SecureDigital direkt mit dem PC oder Laptop verbunden ist, richtet sich die Art und Weise der Geräte-Erkennung nach dem PC- oder Laptop-Modell.

Zulassungseinstellungen für Hybrid Network Bridging

Mit SafeGuard Configuration Protection können Administratoren die gleichzeitige Nutzung verschiedener Netzwerkprotokolle, die zu unabsichtlichem oder absichtlichem Hybrid Network Bridging (z. B. WLAN Bridging und 3G Card Bridging) führen kann, kontrollieren und verhindern. SafeGuard Configuration Protection Clients lassen sich so konfigurieren, dass der Zugang zu WLAN, Bluetooth, Modems oder IrDA-Links blockiert ist, wenn die Haupt-TCP/IP-Netzwerkschnittstelle mit dem Netzwerk verbunden ist. Benutzer können somit die verschiedenen Netzwerkprotokolle nur dann anwenden, wenn sie keine Verbindung zum Netzwerk haben. Dadurch lassen sich Erzeugung und möglicher Missbrauch einer Hybrid Network Bridge vermeiden.

Die Zulassungseinstellungen für Hybrid Network Bridging werden im Bereich *Anti-Hybrid Network Bridging* definiert.

16.3.6 Schritt 5: Gerätekontrolle definieren

Im Bereich *Port-Kontrolle* können Sie für USB-, FireWire- und PCMCIA-Ports festlegen, dass der Zugang zu Ports dieser Art eingeschränkt ist (dies trifft auch für WLAN-Ports zu, siehe *Schritt 7: WLAN-Kontrolle definieren*). Bei Auswahl der Option **Einschränken** können Sie im Bereich **Gerätekontrolle** genauer festlegen, welche Geräte für die betreffenden Ports zugelassen sind.

Im Bereich *Gerätekontrolle* geben Sie an, welche Gerätetypen für den Zugang zugelassen sind. Hier können Sie auch die entsprechende White List zuweisen, in der Sie festlegen, welche Gerätemodelle oder Einzelgeräte zugelassen sind. Wenn ein Gerät unter Anwendung eines der nachfolgend beschriebenen Verfahren als nicht zugelassen definiert ist, wird es gesperrt. Der Bereich Gerätekontrolle einer Richtlinie gilt für **alle** Ports, die **eingeschränkt** sind.

Gerätekontrolle - Einstellungen

- **Alle Geräte** (oberer Bereich):
  Hier können Sie den Zugang für alle Gerätetypen **zulassen**, **einschränken** oder **sperren**. Wenn Sie für **Alle Geräte** die Optionen **Zulassen** oder **Sperren** wählen, wird der Rest dieses Bereichs deaktiviert. Sie können auch Hardware Key Logger zulassen oder sperren.

- **Gerätetypen** (mittlerer Bereich):
  Wenn Sie für **Alle Geräte** die Option **Einschränken** wählen, können Sie den Zugang für ein Gerät nach Typ einschränken. Zum Beispiel: Drucker, Netzwerkadapter oder Audio/Video-Geräte. Die für die Auswahl verfügbaren Gerätetypen sind in SafeGuard Configuration Protection integriert. Wenn Sie ein Gerät eines Typs zulassen möchten, der nicht in der Liste aufgeführt ist, fügen Sie diesen Typ zu Ihrer Liste der zugelassenen Geräte - der **White List** - unter Anwendung der Option **White List für Gerätemodelle** oder **White List für einzelne Geräte** (wie nachfolgend beschrieben) hinzu. Eine Beschreibung der unterstützten Gerätetypen finden Sie im Abschnitt *Unterstützte Gerätetypen*.

- **Unbekannte Geräte** (unterer Bereich):
  Mit dieser Option können Sie festlegen, ob der Zugang zu unbekannten Geräten zugelassen ist oder nicht.

Gerätekontrolle - White List

In diesem Bereich können Sie eine White List für Gerätemodelle und/oder eine White List für einzelne Geräte zuweisen:

- **White List für Gerätemodelle**:
  Diese Option bezieht sich auf ein spezifisches Gerätemodell, z. B. ein bestimmtes HP-Druckermodell wie LaserJet 4050N. Geben Sie eine White List an, die die entsprechenden Angaben enthält.
- **White List für einzelnen Geräte**:
  Diese Option bezieht sich auf einzelne Geräte mit eindeutiger Serienummer, d. h. spezifische Einzelgeräte. Zum Beispiel: der persönliche Drucker des CEO wird zugelassen, andere Drucker nicht. Geben Sie eine White List an, die die entsprechenden Angaben enthält.

Hinweis: Wenn Sie für **Alle Geräte** die Optionen **Zulassen** oder **Sperren** wählen, wird dieser Bereich deaktiviert (siehe *Gerätekontrolle definieren*).

Hinweis: Wenn ein Gerät mehreren Gruppen angehört und diese Gruppen dieselben Zulassungseinstellungen aufweisen, wählt SafeGuard Configuration Protection die Gruppen willkürlich aus.

Gerätekontrolle definieren

1. Legen Sie im Bereich *Alle Geräte* durch Auswahl aus der Dropdownliste fest, ob alle Geräte **zugelassen**, **eingeschränkt** oder **gesperrt** sind.

Hinweis: Wählen Sie **Zulassen** oder **Sperren**, wenn Sie zu diesem Zeitpunkt keine granulare Gerätekontrolle anwenden möchten. Sie können diese Optionen auch dann verwenden, wenn Sie vorhandene granulare Definitionen vorübergehend außer Kraft setzen möchten.

2. Wenn Sie die Optionen **Zulassen** oder **Sperren** für *Alle Geräte* wählen, müssen Sie im Bereich Gerätekontrolle keine weiteren Einstellungen mehr vornehmen und Sie können mit *Schritt 6: Speicherkontrolle definieren* fortfahren.

3. Wenn Sie die Option **Einschränken** für *Alle Geräte* wählen, legen Sie fest, ob Hardware Key Logger **zugelassen** oder **gesperrt** werden sollen.

Hinweis: Wenn der SafeGuard Configuration Protection Client vermutet, dass ein USB Hardware Key Logger an der Tastatur angeschlossen wurde und Hardware Key Logger **gesperrt** sind, wird die Tastatur ebenfalls gesperrt. Um die Tastatur zu aktivieren, muss diese direkt mit dem Computer verbunden werden.

Hinweis: Wenn Sie Hardware Key Logger sperren, werden sowohl USB als auch PS/2 Key Logger gesperrt. Wenn der SafeGuard Configuration Protection Client vor PS/2 Key Logger schützt, werden keine Benutzermeldungen angezeigt. Der Key Logger wird jedoch unbrauchbar, da die Informationen, die er protokolliert, verschlüsselt werden.

Hinweis: Wird ein PS/2 Key Logger bei Benutzung einer PS/2 Keyboard Video Mouse (KVM) gesperrt, so können Sie mit der KVM nicht von der Tastatur aus zwischen Computern wechseln. Dies muss über die KVM selbst erfolgen.

4. Wenn Sie die Option **Einschränken** für *Alle Geräte* wählen, stellen Sie die Zulassungseinstellungen für jeden **Gerätetyp** im Bereich *Gerätetypen* wie folgt ein:

   a) **Zulassen:** Lässt alle Geräte dieses Typs zu.

   b) **Einschränken:** Alle Geräte werden gesperrt, es sei denn, sie werden ausdrücklich in der White List zugelassen (siehe *Geräte und WLAN-Verbindungen zulassen*).

5. Wählen Sie die Optionen **White List für Gerätemodelle** und **White List für einzelne Geräte**, um die zugelassenen Geräte zur White List hinzuzufügen (siehe *Geräte und WLAN-Verbindungen zulassen*).

16.3.7 Schritt 6: Speicherkontrolle definieren

Speichergeräte bilden in der Regel die Hauptkanäle für Informationslecks in einem Unternehmen.

Mit SafeGuard Configuration Protection können Sie den Zugang vollständig zulassen oder jedes Gerät, das als Speichergerät identifiziert wird, sperren. Dies betrifft sowohl Wechselmedien, wie USB-Sticks und Digitalkameras, als auch traditionelle Speichermedien, wie Diskettenlaufwerke, CD/DVD-Laufwerke, externe Festplatten und Magnetbandlaufwerke.

Der Bereich Speicherkontrolle einer Richtlinie wird bei allen Ports, an denen ein Speichergerät angeschlossen werden kann, wirksam. Dies betrifft sowohl **zugelassene** oder **eingeschränkte** Ports als auch Ports, die nicht durch SafeGuard Configuration Protection geschützt sind. Bei einem **gesperrten** Port sind alle Speichergeräte gesperrt, da der Port in diesem Fall nicht mehr zur Verfügung steht.

Hinweis: Da Angriffe und Informationslecks nur sehr selten direkt über interne Festplattenlaufwerke auftreten, lassen sich diese Laufwerke nicht über SafeGuard Configuration Protection sperren oder einschränken, damit der laufende Betrieb nicht beeinträchtigt bzw. unterbrochen wird.

Speicherkontrolle - Einstellungen

Der Bereich Speicherkontrolle umfasst folgende Unterbereiche:

1. **Alle Datenträger** (oberer Bereich):
   Hier können Sie den Zugang zu allen Speichergeräten **zulassen**, **einschränken** oder **sperren**. Wenn Sie für **Alle Datenträger** die Optionen **Zulassen** oder **Sperren** wählen, wird der Rest dieses Bereichs deaktiviert. Sie können auch festlegen, ob die AutoRun-Funktionalität, die auf einigen Datenträgern (z. B. CD/DVD) enthalten ist, gesperrt werden soll.

2. **Speicherarten** (unterer Bereich):
   Wenn Sie die Option **Einschränken** für *Alle Datenträger* gewählt haben, können Sie den Zugang zu einem Datenträger nach Typ einschränken bzw. zulassen. Zum Beispiel: Wechselmedien oder
   CD/DVD. Die für die Auswahl verfügbaren Gerätetypen sind in SafeGuard Configuration Protection integriert. Sie können folgende Gerätetypen und Optionen wählen:

   a) **Wechselmedien:** Betrifft alle Plug-and-Play-Speichergeräte, z. B. USB-Sticks, Digitalkameras MP3 Player usw.

   b) **Smart-Funktionalität von Wechselmedien zulassen:** Wählen Sie die Einstellung Zulassen, um die Verwendung von Wechselmedien, die Smart-Funktionalität implementieren, zuzulassen. Wählen Sie die Einstellung Sperren, um die Smart-Funktionalität solcher Medien zu sperren.

   c) Externe Festplatten

   d) CD/DVD-Laufwerke

   e) Diskettengeräte

   f) Magnetbandgeräte

Wechselmedien, externe Festplatten, CD/DVD-Laufwerke und Diskettenlaufwerke können zusätzlich auf **Schreibgeschützt** gesetzt werden.

Verwenden Sie die *White List*, um die Benutzung spezifischer **Speichermodelle** oder **einzelner Datenträger** zuzulassen. Eine Beschreibung der unterstützten Gerätetypen finden Sie unter *Unterstützte Gerätetypen*. Abschnitt *Speicherkontrolle definieren* beschreibt die Definition von Optionen.

Speicherkontrolle - White List

Hier können Sie eine White List für Speichermodelle und/oder eine White List für einzelne Datenträger zuweisen.

1. **White List für Speichermodelle**:
   Diese Option bezieht sich auf das Modell eines spezifischen Speichergerätetyps, z. B. ein bestimmtes USB-Stick-Modell.

2. **White List für einzelne Datenträger**:
   Einzelne Speichergeräte mit einer eindeutigen Seriennummer, d. h. ein spezifisches Speichergerät. Zum Beispiel: Der persönliche USB-Stick des CEOs wird zugelassen, andere USB-Sticks nicht.

Hinweis: Wenn Sie die Optionen **Zulassen** oder **Blockieren** für *Alle Datenträger* wählen, ist dieser Bereich deaktiviert.

Hinweis: Wählen Sie **Zulassen** oder **Sperren**, wenn Sie zu diesem Zeitpunkt keine granulare Gerätekontrolle anwenden möchten. Sie können diese Optionen auch dann verwenden, wenn Sie vorhandene granulare Definitionen vorübergehend außer Kraft setzen möchten.

16.3.8 Schritt 7: WLAN-Kontrolle definieren

SafeGuard Configuration Protection steuert und überwacht neben Geräten auch WLAN-Verbindungen um sicherzustellen, dass Clients nur autorisierte sichere Verbindungen benutzen. Im Bereich *Port-Kontrolle* können Sie festlegen, dass der Zugang zu einem WLAN-Port **eingeschränkt** ist. Wenn Sie die Option **Einschränken** wählen, können Sie im Bereich **WLAN-Verbindungsarten** genauer festlegen, welche Netzwerke auf den betreffenden Port zugreifen dürfen.

Hinweis: Wenn Sie die Benutzung von WLAN als Port einschränken, überwacht und reguliert SafeGuard Configuration Protection WLAN-Verbindungen über die Microsoft WZC Infrastruktur. Jeder Gerätetreiber, der versucht, ohne Anwendung von WZC auf die Netzwerkkarte zuzugreifen, wird gesperrt.
Wenn Sie eine Reihe von WLAN-Karten verwenden, die proprietäre Treiber in Kraft setzen, können Sie WLAN als Port nur **zulassen** oder **sperren**.

WLAN-Kontrolle - Einstellungen

WLAN-Verbindungsarten:
Mit dieser Option können Sie den Zugang zu WLAN-Netzwerken **zulassen** oder **einschränken** sowie WLAN Peer to Peer Verbindungen **zulassen** oder **einschränken**. Wenn Sie für WLAN-Netzwerke die Option **Einschränken** wählen, können Sie festlegen, welche spezifischen Netzwerke zugelassen sind.

WLAN-Kontrolle - White List

White List für WLAN:
Diese Option bezieht sich auf einzelne Netzwerke einschließlich der Authentisierungs- und Verschlüsselungseigenschaften.

Hinweis: Wenn Sie die Option **Zulassen** für Netzwerke wählen, ist dieser Bereich deaktiviert.

WLAN-Kontrolle definieren

1. Wechseln Sie zur *WLAN*-Option im Bereich **Wireless Ports**. Setzen Sie *WLAN* auf **Einschränken**. Dadurch werden die Optionen unter **WLAN-Verbindungsarten** aktiviert.
2. Definieren Sie im Bereich **WLAN-Verbindungsarten** die Zugangseinstellungen für *Netzwerke (Infrastruktur)* wie folgt:
   a) **Zulassen:** Lässt die Verbindung mit allen WLAN-Netzwerken zu.
   b) **Einschränken:** Alle Netzwerke sind gesperrt, es sei denn, sie sind ausdrücklich in der White List (*siehe Geräte und WLAN-Verbindungen zulassen*) zugelassen.
3. Definieren Sie im Bereich *WLAN-Verbindungsarten* die Zulassungseinstellungen für *Peer to Peer (Ad Hoc)* wie folgt:
   a) **Zulassen:** Lässt Peer to Peer WLAN Verbindungen zu.
   b) **Sperren:** Sperrt alle Peer to Peer WLAN Verbindungen.

Für diese Option stehen keine weiteren granularen Zulassungseinstellungen zur Verfügung.

16.3.9 Schritt 8: Dateikontrolle definieren

Mit SafeGuard Configuration Protection können Sie nicht nur Berechtigungen für Speichergeräte sondern auch für die Dateien, die an und von diesen Geräten übertragen werden, einstellen. Hierzu werden die Dateien beim Transfer an/von externe(n) Speichergeräten auf ihren Typ überprüft. Diese Technologie ermöglicht eine höchst zuverlässige Klassifizierung der Dateien durch Überprüfung des Inhalts des Datei-Headers anstatt der Dateierweiterungen. Der Schutzmechanismus kann somit nicht einfach durch Umbenennen der Dateierweiterung umgangen werden.

Durch die Überprüfung sowohl von Dateien, die von externen Speichergeräten heruntergeladen werden, als auch von Dateien, die auf den geschützten Endpoint hochgeladen werden, lässt sich eine Reihe von Vorteilen erzielen:

- Eine zusätzliche Schutzschicht zur Verhinderung von Daten-Lecks (Data Leakage)
- Schutz vor dem Einbringen von Viren/Malware über externe Speichergeräte.

- Schutz vor dem Einbringen von verbotenen Inhalten über externe Speichergeräte, z. B. nicht lizensierte Software, nicht lizensierte Inhalte (z. B. Musik und Filme), private Inhalte wie private Bilder usw.

Mit dieser Funktion können Sie Richtlinien definieren, die spezifische Dateitypen auf den Kanälen nach innen und nach außen zulassen/sperren.

Die SafeGuard Configuration Protection Dateikontrolle umfasst folgende Funktionalität:

- Dateitypkontrolle - Verfahren zur Kontrolle der Übertragung von Dateien nach deren Typ

Dateikontrolle ist auf Wechselmedien, externe Festplatten und CDs/DVDs anwendbar.

Dateikontrolle - Einstellungen

Dieser Abschnitt enthält folgende Bereiche:

1. **Speicherarten**: In diesem Bereich können Sie die Dateitypkontrolle auf Speicherarten **anwenden** oder Speicherarten von der Dateitypkontrolle **ausnehmen**.
   Die für die Auswahl zur Verfügung stehenden Speicherarten sind in SafeGuard Configuration Protection integriert und umfassen folgende Arten:

   a) **Von Wechselmedien lesen**

   b) **Auf Wechselmedien schreiben**

   c) **Von externen Festplatten lesen**

   d) **Auf externe Festplatten schreiben**

   e) **Von CD/DVD-Medien lesen**

2. Wenn Sie für mindestens eine der Speicherarten **Anwenden** oder **Ausnehmen** wählen, wird der Rest des Abschnitts (Dateitypen) aktiviert. Für jeden Dateityp können Sie die folgenden Berechtigungen einstellen:

   a) **Zulassen**

   b) **Schreibgeschützt**

   c) **Nur schreiben**

   d) **Sperren**
   Die Berechtigungen gelten für alle Speicherarten, auf die Sie die Dateikontrolle im Abschnitt *Speicherarten* angewendet haben.

Die folgende Tabelle bietet eine Auflistung der Dateitypen und Dateierweiterungen, die von der SafeGuard Configuration Protection Dateitypkontrolle unterstützt werden.

Dateityp	Erweiterungen	Beschreibung
Microsoft Office	DOC	Microsoft Word Dokument
	DOCX	Microsoft Word Dokument
	DOCM	Microsoft Word Dokument
	DOT	Microsoft Word Dokumentvorlage
	DOTX	Microsoft Word Dokumentvorlage
	DOTM	Microsoft Word Dokumentvorlage
	RTF	Rich Text Format
	PPT	Microsoft PowerPoint Präsentation
	PPTX	Microsoft PowerPoint Präsentation
	PPTM	Microsoft PowerPoint Präsentation
	POT	Microsoft PowerPoint Vorlage
	POTX	Microsoft PowerPoint Vorlage
	POTM	Microsoft PowerPoint Vorlage
	PPS	Microsoft PowerPoint Show
	PPSX	Microsoft PowerPoint Show
	PPSM	Microsoft PowerPoint Show
	PPA	Microsoft PowerPoint Add-In
	PPAM	Microsoft PowerPoint Add-In
	XLS	Microsoft Excel Arbeitsmappe
	XLSX	Microsoft Excel Arbeitsmappe
	XLSM	Microsoft Excel Arbeitsmappe
	XLSB	Microsoft Excel Arbeitsmappe
	XLT	Microsoft Excel Vorlage
	XLTX	Microsoft Excel Vorlage
	XLTM	Microsoft Excel Vorlage
	XLA	Microsoft Excel Add-In
	XLAM	Microsoft Excel Add-In
	MPP	Microsoft Project Projekt

	MPT	Microsoft Project Vorlage
	VSD	Microsoft Visio Zeichnung
	VDX	Microsoft Visio Zeichnung
	VSS	Microsoft Visio Schablone
	VSX	Microsoft Visio Schablone
	VST	Microsoft Visio Vorlage
	VTX	Microsoft Visio Vorlage
	PUB	Microsoft Publisher
	ONE	Microsoft OneNote Abschnitt
	ADP	Microsoft Access Projekt
	ADE	Microsoft Access Projekterweiterung
Publizierte Dokumente	PDF	Adobe Acrobat Dokument
	PS	Post Script Dokument
	EPS	Encapsulated Post Script
Web-Seiten	HTML	HTML Web-Seite
	HTM	HTML Web-Seite
	MHT	Archivierte Web-Seite
	MHTML	Archivierte Web-Seite
	PHP	PHP Skript
	HLP	Windows Hilfedateien
	CHM	Kompilierte Hilfedateien
	ASP	Active Server Page
	ASPX	ASP.NET Web-Seite
	ASMX	ASP.NET Webservices
	JHTML	Java HTML Web-Seite
	JSP	Java Server Page
Bilder	JPG	JPEG Bild
	JPEG	JPEG Bild
	GIF	GIF Bild
	BMP	Bitmap Bild
	DIB	Device Independent Bitmap Bild

	PNG	PNG Bild
	TIF	Tagged Image Format
	TIFF	Tagged Image Format
	MDI	Office Document Imaging Datei
	JNG	JNG Bild
	MNG	MNG Bild
	ICO	Windows Symbol
	CUR	Windows Cursor
	WMF	Windows Metafile Bild
	EMF	Enhanced Windows Metafile Bild
	FH9	Macromedia Freehand 9 Grafiken
	JP2	JPEG-2000 Bild
	PBM	Portable Bitmap
	PGM	Portable Graymap Bitmap
	PPM	Portable Pixelmap Bitmap
	PSD	Adobe Photoshop Grafiken
	CDR	CorelDRAW Vector Grafiken
	SVG	Scalable Vector Graphics
Multimedia	WAV	Waveform Audio
	WMA	Windows Media Audio
	MP2	MPEG Audio
	MP3	MPEG Audio
	AIFF	Audio Interchange
	AIF	Audio Interchange
	AU	AU Audio
	RA	RealMedia Streaming Media
	MID	Musical Instrument Digital Sound
	MIDI	Musical Instrument Digital Sound
	RMI	Musical Instrument Digital Sound
	SDS	Musical Instrument Digital Sound Sample
	VOC	Creative Lab's Soundblaster Audio

	OGG	Ogg Vorbis Codec Audio
	VOX	Dialogic Audio
	FLAC	Free Loseless Codec Audio
	MPEG	MPEG Multimedia
	MPG	MPEG Multimedia
	AVI	Audio Video Interleave
	ASF	Advanced Streaming Format
	WMV	Windows Media Multimedia
	MOV	QuickTime Video Clip
	SWF	Flash Animationsdatei
	FLI	FLIC Animation
	FLC	FLIC Animation
Text & Programmcode	TXT	Textdatei
	CSV	Formatierter Text (durch Kommas getrennt)
	PRN	Formatted Text (durch Leerzeichen getrennt)
	CPP	C++ Programmcode
	C	C/C++ Programmcode
	H	C/Java Header-Datei
	XML	XML-Datei
	F	FORTRAN Programmcode
	T90	FORTRAN Programmcode
	MAKEFILE	Kompilierungssteuerungdatei
	MAKEFILE.IN	Kompilierungssteuerungdatei
	PL1	PL1 Programmcode
	ASM	Assembler Programmcode
	PAS	PASCAL Programmcode
	JAVA	JAVA Programmcode
	M4	Meta4 Programmcode
	BCPL	BCPL Programmcode
	CS	Visual C#.NET Programmcode
	PL	Perl Programmcode

	PM	Perl Programmcode Modul
	PY	Python Programmcode
	PDB	Visual C++/.NET Programmdatenbank
	BAS	BASIC Programmcode
	VB	Visual Basic Programmcode
	VBS	VBScript Skript
	JS	JavaScript Source Code
Ausführbare Dateien	EXE	Ausführbare Datei
	DLL	Dynamic Link Library
	PIF	Windows Program Information Datei
	BAT	Batch
	COM	Befehl
	OCX	ActiveX - Object Linking and Embedding (OLE) Control Erweiterung
	CMD	Befehl
	CPL	Windows Systemsteuerung-Erweiterung
	SCR	Windows Bildschirmschoner
	VXD	Virtual Device Treiber
	SYS	System Device Treiber
	CLASS	Java Bytcode
	PYC	Python Compiler Skript (Bytecode)
	LIB	Program Library Common Object File Format (COFF), Dateiformat für allgemeines Objekt
	INS	InstallShield Skript
	OBJ	Objektdatei
	O	Objektdatei
Komprimierte Archive	ZIP	ZIP-komprimiertes Archiv
	ARJ	ARJ-komprimiertes Archiv
	RAR	WinRAR-komprimiertes Archiv
	GZIP	GZIP-komprimiertes Archiv
	TAR	Bandarchiv

	JAR	JAR-komprimiertes Archiv
	ACE	WinAce-komprimiertes Archiv
	HQX	Macintosh BinHex 4-komprimiertes Archiv
	LZH	LHA-komprimiertes Archiv
	LHA	LHA-komprimiertes Archiv
	AR	AIX Small Indexed Archiv
	ARC	LH ARC-komprimiertes Archiv
	CAB	Cabinet-komprimiertes Archiv
	**_	Komprimierte Installationsdateien (z. B. EX_, DL_)
CD/DVD Disc Images	ISO	ISO Disc Image
	BIN	BIN Disc Image
	CIF	EasyCD Creator Disc Image
	CCD	CloneCD Disc Image
	IMG	CloneCD Disc Image
	MDF	Alcohol 120% Disc Image
	DAA	PowerISO Disc Image
	C2D	WinOnCD Disc Image
Databanken	MDB	Microsoft Access Datenbank
	ACCDB	Microsoft Access Datenbank
	ACCDT	Microsoft Access Datenbankvorlage
	MDA	Microsoft Access Add-In
	MDW	Microsoft Access Arbeitsgruppe
	MDE	Microsoft Access - kompilierte Datenbank
	MYD	MySQL MyISAM Datenbank
	MYI	MySQL MyISAM Datenbank-Index
	FRM	MySQL MyISAM Generic Dictionary
	DBF	dBase Datenbank
	DBT	Microsoft FoxPro Datenbank
	GDB	Borland InterBase Datenbank
	PX	Paradox Datenbank

Microsoft Outlook	PST	Outlook - persönlicher Ordner
	DBX	Outlook Express E-Mail-Ordner
PGP Verschlüsselung	PGP	Pretty Good Privacy (PGP) Encrypted
	ASC	Pretty Good Privacy (PGP) Armored Encrypted
	CTX	Pretty Good Privacy (PGP) Ciphertext
Computer-Aided Design (CAD)	DWG	AutoCAD Zeichnung
	DXF	AutoCAD Interchange
	ASM	Pro/ENGINEER Assembly
	PRT	Pro/ENGINEER Modell
Adobe FrameMaker	DOC	Adobe FrameMaker/FrameBuilder Dokument
	FM	Adobe FrameMaker Dokument
	FRM	Adobe FrameMaker Dokument
	BOOK	Adobe FrameMaker Buch
	MIF	Adobe FrameMaker Austauschformat

16.3.10 Schritt 9: Richtlinie speichern und veröffentlichen

Richtlinien werden wie für alle anderen Richtlinien beschrieben gespeichert und veröffentlicht.

16.4 White Lists - Geräte und WLAN-Verbindungen zulassen

Die Beschreibungen in den folgenden Abschnitten beziehen sich auf das Hinzufügen von zugelassenen Geräten zu einer White List vom Typ *Gerätekontrolle* sowie auf das Hinzufügen von zugelassenen Speichermedien zu einer White List vom Typ *Speicherkontrolle*. Unterschiede beim Hinzufügen von Speichergeräten und anderen Geräte werden gesondert hervorgehoben und beschrieben.

Das Hinzufügen von zugelassenen WLAN-Netzwerken ist im Abschnitt *WLAN-Verbindungen hinzufügen* beschrieben.

SafeGuard Configuration Protection bietet drei Berechtigungsebenen:

- **Gerätetypen und Speicherarten:**
  Über diese Optionen können Sie den Zugang zu einem Endgerät in Abhängigkeit vom angeschlossenen Gerätetyp zulassen oder einschränken. Zum Beispiel: Wechselmedien, Netzwerkadapater, Eingabegeräte (HID, z. B. Maus) oder Bildverarbeitungsgeräte. Die für die Auswahl verfügbaren Gerätetypen und Speicherarten sind in SafeGuard Configuration Protection integriert und befinden sich in den beschriebenen Bereichen *Gerätekontrolle* und *Speicherkontrolle*.
  Ein Gerätetyp kann **zugelassen** (Default) **gesperrt** oder **eingeschränkt** sein. Wenn Sie einen Gerätetyp **einschränken**, werden alle Geräte dieses Typs gesperrt, es sei denn, sie sind ausdrücklich in einer White List als zugelassen definiert.

- **White List für Gerätemodelle:** Diese Option bezieht sich auf das Zulassen von Geräte- oder Speichermodellen, z. B. alle HP-Drucker oder alle M-Systems USB-Sticks.

- **White List für einzelne Geräte:** Diese Option bezieht sich auf das Zulassen von einzelnen Geräten oder Speichergeräten mit eindeutiger Seriennummer, d. h. spezifische Einzelgeräte. Wenn z. B. die Verwendung des USB-Sticks des CEO zugelassen werden soll, alle anderen USB-Sticks jedoch gesperrt sein sollen, setzen Sie die Speicherart **Wechselmedien** auf **Einschränken** und geben Sie die kennzeichnenden Parameter des USB-Sticks des CEO in einer White List für einzelne Datenträger ein.

Dieser Abschnitt beschreibt folgende Vorgänge:

- Anlegen einer White List

- Hinzufügen von zugelassenen Modellen oder einzelnen Geräten zu einer White List.
  Als Grundlage dient hier entweder die Liste mit Geräten, deren Verwendung von SafeGuard PortAuditor erkannt wurde, oder eine manuell erstellte Liste.

16.4.1 White Lists anlegen

So registrieren Sie eine White List:

1. Markieren Sie **White List** im Richtlinien-Navigationsbereich.
2. Klicken Sie im Kontextmenü des Eintrags auf **Neu > White List**.
3. Geben Sie unter **Name der White List** einen Namen ein.
4. **Typ der White List auswählen**

   White Lists können angelegt werden für:

   - Gerätemodelle
   - Einzelne Geräte
   - Datenträgermodelle
   - Einzelne Datenträger
   - WLAN-Netzwerke

   Die einzelnen White Lists können dann bei den Richtlinieneinstellungen ausgewählt werden.
5. Wählen Sie aus, ob Sie die White List manuell erstellen wollen oder ob als Quelle das Ergebnis eines Scans Ihrer Computer durch SafeGuard PortAuditor verwendet werden soll.

Hinweis: Die Ergebnisse des Scans durch SafeGuard PortAuditor müssen vorliegen (XML-Datei), wenn Sie die White List auf diese Weise erzeugen wollen.

a) **White List manuell erstellen**
Haben Sie diese Option gewählt, wird nach dem Klicken auf **OK** eine leere White List im SafeGuard Management Center geöffnet, in der Sie manuell Einträge erstellen können.

b) **SafeGuard PortAuditor Ergebnis importieren**
Wenn Sie diese Option wählen, wird das Ergebnis eines Scans durch SafeGuard PortAuditor importiert.

- Sie können dann die von SafeGuard PortAuditor zur Verfügung gestellte Datei über die Schaltfläche **[...]** auswählen.
- Nach dem Klicken auf **OK** wird der Inhalt der importierten Datei im SafeGuard Management Center angezeigt

16.4.2 Gerät unter Benutzung einer SafeGuard PortAuditor Datei hinzufügen

Voraussetzung: Erstellen einer Geräteinformationsdatei

Um eine Datei zu erstellen, die Informationen zu den Geräten, die Sie zulassen möchten, enthält, verwenden Sie SafeGuard PortAuditor zum Scannen der betreffenden Computer. SafeGuard PortAuditor scannt die ausgewählten Computer und liefert Informationen zu allen Geräten und WLAN-Netzwerken, die derzeit mit diesen Computern verbunden sind, bzw. zu einem früheren Zeitpunkt mit ihm verbunden waren. Die Ergebnisse dieses Prüfvorgangs werden in einer XML-Datei gespeichert, Weitere Informationen zu SafeGuard PortAuditor finden Sie im *SafeGuard PortAuditor 3.2 User Guide*.

16.4.2.1 Schritt 1: Geräteinformationen abrufen

In diesem Schritt geben Sie die Datei an, aus der die Informationen zu den Geräten, die hinzugefügt werden, entnommen werden. Das heißt, Sie geben den Speicherort der SafeGuard PortAuditor .XML-Datei an, die die erforderlichen Geräteinformationen enthält. Nachdem Sie die erforderliche Datei über die Schaltfläche **[...]** ausgewählt haben, klicken Sie auf **OK** um fortzufahren.

16.4.2.2 Schritt 2: Geräte auswählen

In Schritt 2 wird eine Tabelle mit den Geräten, die bei den Endgeräten in Ihrem Netzwerk ermittelt wurden, angezeigt. Hier können Sie die Geräte auswählen, die zur White List hinzugefügt werden sollen. Die Tabelle ist in Kategorien unterteilt. Die Kategorien richten sich danach, ob Sie Geräte zu einer White List für Gerätemodelle oder einer White List für Einzelgeräte hinzufügen und ob Sie Speichergeräte oder Nicht-Speichergeräte hinzufügen.

Neben auswählbaren Geräten wird ein Kontrollkästchen angezeigt. Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Gerätemodell oder das Einzelgerät zulassen möchten. Sie können alle markierten Geräte auswählen, bzw. die Auswahl aufheben, indem Sie in der Tabelle mit der rechten Maustaste klicken.

Hinweis: Speichergeräte können nicht zu einer *Gerätekontrolle* White List hinzugefügt werden.

Hinweis: Geräte oder Speichergeräte ohne eindeutige Kennung können nicht zu einer *Einzelgeräte* White List hinzugefügt werden.

Gelegentlich wird ein Gerät von SafeGuard PortAuditor nicht als Speichergerät identifiziert. Dies kann zum Beispiel der Fall sein, wenn vom Hersteller keine Geräteklasse eingebettet wurde. In diesem Fall können Sie das betreffende Gerät, wenn es sich tatsächlich um ein Speichergerät handelt, zur White List für Speichergeräte Ihrer Richtlinie hinzufügen.

Speichergeräte dürfen nicht zu einer *Gerätekontrolle* White List hinzugefügt werden. Ebenso dürfen keine Nicht-Speichergeräte zu einer *Speicherkontrolle* White List hinzugefügt werden. In diesen beiden Fällen ignoriert der SafeGuard Configuration Protection Client die hinzugefügten Geräte.

Hinweis: Wenn Sie ein Gerät hinzufügen, das sich bereits auf einer anderen Geräte White List in der betreffenden Richtlinie befindet, und die Zulassungen in den White Lists unterscheiden sich voneinander, so gilt die White List, die mehr zulässt.

16.4.2.3 Schritt 3: White List speichern

Speichern Sie die White List durch Klicken auf das Symbol in der SafeGuard Enterprise Symbolleiste.

Mit der **Inhalt ändern** Schaltfläche können Sie den Inhalt aus einer anderen Datei in die White List einfügen. Neue Einträge werden am Ende der White List hinzugefügt.

16.4.3 Gerät manuell hinzufügen

Wenn Sie eine leere White List angelegt haben, müssen Sie die Einträge manuell erstellen.

Wenn Sie Geräte zu einer bereits vorhandenen White List hinzufügen möchten, z. B. Geräte, die nicht mit einem Endgerät in Ihrem Unternehmen verbunden waren und somit nicht in den Prüfergebnissen von SafeGuard PortAuditor erscheinen, müssen Sie diese Geräte ebenfalls manuell hinzufügen.

Die folgenden Handlungsschritte gelten sowohl für das Hinzufügen von Speichergeräten (in *Speicherkontrolle*) als auch für das Hinzufügen von Nicht-Speichergeräten (in *Gerätekontrolle*).

Hinweis: Wenn Sie ein Gerät hinzufügen, das sich bereits auf einer anderen Geräte White List in der betreffenden Richtlinie befindet, und die Zulassungen in den White Lists unterscheiden sich voneinander, so gilt die White List, die mehr zulässt.

So fügen Sie ein Gerät manuell zu einer White List hinzu:

1. Klicken Sie auf das Symbol in der SafeGuard Enterprise Symbolleiste, um einen neuen Eintrag zur White List hinzuzufügen.
2. Geben Sie in den folgenden Feldern die erforderlichen Informationen ein:
   a) **Port** – optional
   b) **Beschreibung** – optional
   c) **Geräte-Information** – optional
   d) **Hersteller (Hersteller-ID)** – optional
   e) **Produkt (Produkt-ID)** – optional
   f) **Hardware-ID/Instanz-ID** – **erforderlich**

Stellen Sie sicher, dass Sie in allen Feldern die korrekten Daten eingegeben haben und **speichern** Sie die White List.

Um einen Eintrag aus der White List zu entfernen, wählen Sie den Eintrag aus und klicken Sie auf das Symbol in der SafeGuard Enterprise Symbolleiste.

Hinweis: Die Hersteller-ID (VID), Produkt-ID (PID), die Hardware-ID (HID) sowie die Instanz-ID (IID) finden Sie in den SafeGuard PortAuditor Scan-Ergebnissen, auf einem Aufkleber auf dem Produkt selbst oder im Windows Geräte-Manager.

16.4.4 WLAN-Verbindungen hinzufügen

WLAN-Verbindungen werden zur *WLAN-Netzwerk* White List auf die gleiche Art und Weise hinzugefügt, wie Geräte zu den entsprechenden White Lists. Erstellen Sie eine WLAN White List und fügen Sie dann die zugelassenen Verbindungen unter Anwendung der SafeGuard PortAuditor Datei oder manuell hinzu.

16.4.4.1 WLAN-Verbindung manuell hinzufügen

WLAN-Verbindungen, die nicht von SafeGuard PortAuditor erkannt wurden und somit nicht über den Importmechanismus hinzugefügt werden können, lassen sich manuell zu einer White List hinzufügen.

WLAN-Netzwerkinformationen eingeben

An dieser Stelle definieren Sie die Parameter, denen ein Netzwerk entsprechen muss, um zugelassen zu werden. Sie können ein Netzwerk mit seinem Namen oder seiner MAC-Adresse spezifizieren. Nach der Eingabe eines Netzwerknamens oder einer MAC-Adresse können Sie auch die Authentisierungs- und Datenverschlüsselungsparameter angeben, die übereinstimmen müssen. Nur Netzwerke, die allen Parametern entsprechen, werden zugelassen.

So fügen Sie eine WLAN-Verbindung manuell zu einer White List hinzu:

1. Öffnen Sie die White List für WLAN-Verbindungen.
2. Klicken Sie auf das Symbol in der SafeGuard Enterprise Symbolleiste, um einen neuen Eintrag zur White List hinzuzufügen.
3. Geben Sie den **Netzwerknamen**, die **MAC-Adresse** oder beide Angaben ein. Mindestens ein Feld muss ausgefüllt werden.
4. Wenn Sie nur den **Netzwerknamen** angeben möchten, geben Sie den Namen ein und fahren Sie mit Schritt 6 fort.
5. Wenn Sie nur die **MAC-Adresse** angeben möchten, geben Sie die Adresse ein und fahren Sie mit Schritt 6 fort.
6. Um Sicherheitseinstellungen zu definieren, spezifizieren Sie die erforderlichen Einstellungen für **Netzwerkauthentisierung** und **Datenverschlüsselung** durch Auswahl aus den Dropdownlisten. Angaben in diesen Feldern sind optional.

Hinweis: Die in der Dropdownliste verfügbaren Optionen für die **Datenverschlüsselung** richten sich nach dem ausgewähltenTyp der **Netzwerkauthentisierung**. Für WPA-Netzwerkauthentisierung stehen zum Beispiel die Verschlüsselungsoptionen TKIP und AES zur Verfügung. Für die 802.1X-Authentisierung dagegen nur die Option WEP.

7. Stellen Sie sicher, dass Sie in allen Feldern die korrekten Daten eingegeben haben und speichern Sie die White List.

16.5 Unterstützte Gerätetypen

Dieses Kapitel liefert eine Auflistung der Gerätetypen, die SafeGuard Configuration Protection beim Erstellen einer Richtlinie für die Auswahl zur Verfügung stellt.

Für **Nicht-Speichergeräte** können Sie die Verwendung von Geräten an USB-, FireWire- und PCMCIA-Ports einschränken. SafeGuard Configuration Protection bietet im *Gerätekontrolle*-Bereich eine Auswahl an integrierten Gerätetypen für die Definition von zugelassenen oder gesperrten Gerätetypen. Wenn Sie einen Gerätetyp benötigen, der hier nicht aufgelistet ist, verwenden Sie die Funktion zur Einschränkung von Einzelgeräten (siehe *Geräte und WLAN-Verbindungen zulassen*).

Für **Speichergeräte** erkennt SafeGuard PortAuditor in den meisten Fällen durch Identifizieren des Volume oder unter Verwendung der eingebetteten Klassendaten, ob es sich um ein Speichergerät oder ein Nicht-Speichergerät handelt. Dadurch wird eine Kategorisierung von Gerätelisten nach Speichergeräten und einfachen (Nicht-)Speichergeräten für Ihre Auswahl ermöglicht. Sie erhalten somit eine Hilfestellung bei der Definition Ihrer Richtlinie. SafeGuard Configuration Protection bietet eine Auswahl an integrierten Typen im Bereich *Speicherkontrolle*, mit deren Hilfe Sie festlegen können, welche Gerätetypen zugelassen oder gesperrt werden sollen.

Die folgenden Gerätetypenlisten sind in Nicht-Speichergeräte und Speichergeräte aufgeteilt.

16.5.1 Nicht-Speichergeräte-Typen

Dieser Abschnitt liefert eine Auflistung der integrierten Nicht-Speichergerätetypen, für die in SafeGuard Configuration Protection eine Richtlinie definiert werden kann.

Hinweis: Die Gerätekontrolle für Nicht-Speichergeräte kann nur für USB-, FireWire- und PCMCIA-Ports definiert werden.

1. **Eingabegeräte (Human Interface Devices, HID)**
   Geräte zur Steuerung und Benutzung von Computersystemen. Typische Beispiele: Tastaturen, Steuerungsgeräte wie Maus, Steuerungsball und Joystick.

2. **Drucker**
   Über USB, PCMCIA oder FireWire angeschlossene Drucker

3. **Personal Data Assistants (PDAs)**
   Diese umfassen:

   a) Windows Mobile Geräte/Pocket PC-Geräte

   b) Blackberry-Geräte

   c) Palm OS Geräte

4. **Mobiltelefone**
   Neue Mobiltelefonmodelle, die für USB als „Wireless USB Devices“ eingestuft sind.

5. **Netzwerkadapter**
   Kommunikationsgeräte, z. B. Ethernet-Netzwerkadapter, WiFi-Adapter, ADSL- und Kabel-Modems mit USB-Verbindung.

6. **Bildverarbeitungsgeräte**
   In erster Linie Geräte wie Scanner und Digitalfotokameras.

7. **Audio-/Videogeräte**
   Zum Beispiel: Mikrofone, Telefone, Lautstärkeregler, Web-Kameras, digitale Camcorder, digitale TV-Karten sowie Digitalfotokameras mit Video-Streaming-Unterstützung.

8. **Smartcards**
   Smartcard-Geräte

9. **Content Security Devices**
   Zur Bereitstellung spezieller Sicherheitsfunktionen, z. B. verstärkte Authentisierung, biometrische Identifizierung und Software-Lizensierung.

16.5.2 Speichergerätetypen

Der Speichergeräteschutz bezieht sich auf alle nicht gesperrten Ports. Das heißt, es spielt keine Rolle, an welchem Port das Speichergerät angeschlossen ist, solange der betreffende Port nicht als gesperrt definiert ist.

Hinweis: Die Gerätekontrolle für Speicherkontrolle kann für jeden Port-Typ, auch zum Beispiel für Parallel-Ports, USB-, FireWire- und PCMCIA-Ports, definiert werden.

Die nachfolgend aufgelisteten integrierten Gerätetypen werden von SafeGuard Configuration Protection unterstützt.

- **Wechselmedien**
  Wechselmedien umfassen Nur-Speichergeräte, z. B. disk-on-key, USB-Sticks und SD Flash Cards und Geräte, die einen einzigartigen Anwendungszweck haben, jedoch vom Computer als neues Speicherlaufwerk angesehen werden, z. B. MP3 Player, Digitalkameras und PDAs.
- **Externe Festplatten**
  Extern (z. B. über USB) angeschlossene Festplatten
- **CD/DVD-Laufwerke**
  Sowohl integriert als auch extern angeschlossen
- **Diskettenlaufwerke**
  Sowohl integriert als auch extern angeschlossen
- **Magnetbandlaufwerke**
  Sowohl integriert als auch extern angeschlossen

17 Benutzer-Computer Zuordnung

SafeGuard Enterprise verwaltet die Informationen, welcher Benutzer sich an welchem Computer anmelden darf, in einer Liste, für die in der Folge der Begriff UMA (für User-Machine-Assignment) verwendet wird.

Voraussetzung für die Aufnahme in die UMA ist, dass sich der Benutzer einmal an einem Computer mit installiertem SafeGuard Enterprise angemeldet hat und als „kompletter" Benutzer, im Sinne von SafeGuard Enterprise, im SafeGuard Management Center vorhanden ist. Als „komplett" wird ein Benutzer dann bezeichnet, wenn für ihn nach der ersten Anmeldung ein Zertifikat erzeugt und danach sein Schlüsselring aufgebaut wurde. Erst dann ist die Möglichkeit gegeben, dass diese Benutzerdaten auch auf andere Computer repliziert werden können. Nach der Replikation kann sich der Benutzer auch auf diesen Computern in der POA anmelden.

In der Standardeinstellung wird der erste Benutzer, der sich nach der Installation von SafeGuard Enterprise an den Benutzer-Computer anmeldet, in der UMA als Besitzer dieses Computers eingetragen.

Dieses Attribut erlaubt es dem Benutzer, nachdem er sich im Rahmen der Power-on Authentication authentisiert hat, weiteren Benutzern die Anmeldung an diesem Computer zu ermöglichen, siehe *Weitere Benutzer importieren* auf Seite 203. Dadurch werden auch sie in die UMA für diesen Computer aufgenommen.

So wird automatisch eine Liste aufgebaut, die bestimmt, welcher Benutzer sich an welchem Computer anmelden darf. Diese Liste kann im SafeGuard Management Center bearbeitet werden.

17.1 Benutzer-Computer Zuordnung im SafeGuard Management Center

Im SafeGuard Management Center kann eine Zuweisung von Benutzern zu bestimmten Computern vorgenommen werden. Wird ein Benutzer im SafeGuard Management Center einem Computer zugeordnet (oder umgekehrt), wird diese Zuweisung in die UMA aufgenommen. Seine Benutzerdaten (Zertifikat, Schlüssel usw.) werden auf diesen Rechner repliziert, und er kann sich an diesen Computer anmelden.

Im Rahmen dieser Zuordnung kann auch festgelegt bzw. geändert werden, wem es erlaubt ist, weiteren Benutzern die Anmeldung an diesen Computer zu ermöglichen.

Unter **Typ** wird angezeigt, wie der Benutzer in die SafeGuard Enterprise Datenbank aufgenommen wurde. **Übernommen** gibt an, dass der Benutzer auf einem Client in die UMA für den Computer aufgenommen worden ist.

Hinweis: Wird im SafeGuard Management Center keine Zuweisung vorgenommen und kein Benutzer als Besitzer festgelegt, wird der Benutzer, der sich als erster nach der Installation von SafeGuard Enterprise an den Benutzer-Computer anmeldet, als Besitzer eingetragen. Dieser Benutzer kann dann weiteren Benutzern die Anmeldung an diesen Computer ermöglichen, siehe *Weitere Benutzer importieren* auf Seite 203.
Werden im Management Center diesem Computer nachträglich Benutzer zugewiesen, so können sich diese dann auch in der Power-On Authentication anmelden. Voraussetzung dafür ist allerdings, dass es sich um komplette Benutzer (deren Zertifikat und Schlüssel bereits existieren) handelt.
Die Erlaubnis durch den Besitzer des Computers ist dann nicht notwendig.

Über folgende Einstellungen kann festgelegt werden, wem es erlaubt ist, weitere Benutzer in die UMA aufzunehmen:

- **Kann Besitzer werden:**
  Die Aktivierung dieser Einstellung ist Voraussetzung dafür, dass ein Benutzer als Besitzer eines Computers eingetragen werden kann.

- **Benutzer ist Besitzer:**
  Ist diese Einstellung ausgewählt, wird dieser Benutzer als Besitzer in die UMA eingetragen. Er kann weitere Benutzer in die UMA aufnehmen. Es kann jeweils nur ein Benutzer pro Computer als Besitzer in der UMA eingetragen werden.

Wer Benutzer in die UMA aufnehmen darf, wird zusätzlich über die Richtlinieneinstellung **Importieren von neuen Benutzern erlaubt für** in einer Richtlinie vom Typ **Spezifische Computereinstellungen** gesteuert.

- **Importieren von Benutzern erlaubt für**

  Niemand:
  Auch der als Besitzer eingetragene Benutzer kann keinen weiteren Benutzern die Aufnahme in die UMA ermöglichen. Die Funktionalität, dass ein Besitzer weitere Aufnahmen ermöglichen kann, wird damit ausgeschaltet.

  Besitzer (Standardeinstellung):
  Nur der Besitzer kann weitere Benutzer in die UMA aufnehmen

Hinweis: Ein Sicherheitsbeauftragter kann im SafeGuard Management Center immer Benutzer hinzufügen.

  Jeder:
  Hebt die Einschränkung auf, dass nur der Besitzer Benutzer hinzufügen darf.

Beispiel:
Das folgende Beispiel zeigt, wie Sie im SafeGuard Management Center festlegen können, dass sich ausschließlich drei bestimmte Benutzer (Benutzer_a, Benutzer_b, Benutzer_c) auf dem Computer Computer_ABC anmelden können.

Ausgangssituation:
Sie legen im SafeGuard Management Center das gewünschte Verhalten fest. SafeGuard Enterprise wird in der Nacht auf allen Benutzer-PCs installiert. Am Morgen sollen sich die Benutzer entsprechend Ihren Vorgaben anmelden.

1. Weisen Sie im SafeGuard Management Center Benutzer_a, Benutzer_b, Benutzer_c dem Computer Computer_ABC zu. (Benutzer & Computer -> Computer_ABC auswählen -> Benutzer via Drag&Drop zuweisen). Damit haben Sie eine UMA festgelegt.

2. Setzen Sie in einer Computerrichtlinie die Einstellung Importieren von neuen Benutzern erlaubt für auf Niemand.
   Da es Benutzer_a, Benutzer_b, Benutzer_c nicht erlaubt werden soll, Benutzer hinzuzufügen, ist es nicht notwendig, einen Benutzer als Besitzer festzulegen.

3. Weisen Sie die Richtlinie dem Computer zu bzw. an einer Stelle in der Verzeichnisstruktur zu, wo sie für den Computer wirksam wird.

Bei der Anmeldung des ersten Benutzers an Computer_ABC (siehe *Ablauf der Anmeldung* auf Seite 201), wird ein Autologon für die POA ausgeführt. Die Computerrichtlinien werden an den Benutzer-Computer geschickt. Da Benutzer_a in der UMA eingetragen ist, wird er im Zuge der Windows-Anmeldung komplettiert. Seine Benutzerrichtlinien, Zertifikate und Schlüssel werden an den Endpoint-Computer geschickt. Die POA wird aktiviert.

Hinweis:
Der Benutzer kann über die Statusausgabe im SafeGuard Tray Icon überprüfen, wann dieser Vorgang abgeschlossen ist.

Benutzer_a existiert nun als kompletter Benutzer in SafeGuard Enterprise und kann sich bei der nächsten Anmeldung in der POA authentisieren und wird automatisch angemeldet.

Benutzer_a fährt nun den Computer herunter und Benutzer_b will sich anmelden. Da die POA aktiviert ist, findet kein Autologon mehr statt.

Für die Benutzer_b und Benutzer_c gibt es nun zwei Möglichkeiten, Zugang zu diesem Computer zu erlangen.

a) Benutzer_a deaktiviert im POA-Anmeldedialog die Option Durchgehende Anmeldung an Windows und meldet sich an.

b) Benutzer_b authentisiert sich über Challenge/Response in der POA.

In beiden Fällen wird anschließend der Windows-Anmeldedialog angezeigt.

Benutzer_b kann dort seine Windows-Anmeldeinformationen eingeben. Seine Benutzerrichtlinien, Zertifikate und Schlüssel werden an den Benutzer-Computer geschickt. Er wird in der POA aktiviert. Benutzer_b existiert nun als kompletter Benutzer in SafeGuard Enterprise. Er kann sich bei der nächsten Anmeldung in der POA authentisieren und wird automatisch angemeldet.

Es wurde in der Computerrichtlinie zwar festgelegt, dass auf diesem Computer niemand Benutzer importieren darf, da sie sich aber bereits in der UMA befinden, können Benutzer_b und Benutzer_c durch die Windows-Anmeldung dennoch komplettiert und in der POA aktiviert werden.

Alle anderen Benutzer werden nicht in die UMA aufgenommen und können sich daher niemals an der Power-on Authentication authentisieren. Alle Benutzer, die sich an Windows anmelden und nicht Benutzer_a, Benutzer_b oder Benutzer_c sind, werden in diesem Szenario nicht in die UMA aufgenommen und daher auch nie in der POA aktiv.

Sie können im SafeGuard Management Center später weitere Benutzer hinzufügen. Diese Benutzer können sich an Computer_ABC anmelden. Allerdings steht ihr Schlüsselring nach der ersten Anmeldung noch nicht zur Verfügung, da eine Synchronisierung erst durch diese Anmeldung angestoßen wird. Nach einer erneuten Anmeldung steht auch der Schlüsselring zur Verfügung und die Benutzer können entsprechend den geltenden Richtlinien auf den Computer zugreifen. Haben sie sich zuvor noch an keinem Benutzer-Computer erfolgreich angemeldet, können sie wie zuvor beschrieben aufgenommen werden.

Benutzer sperren

Durch Aktivieren des Kontrollkästchens in der Spalte **Benutzer sperren** wird dem Benutzer die Anmeldung an diesem Computer verboten. Darüberhinaus wird der Computer automatisch heruntergefahren wenn der betreffende Benutzer angemeldet ist, wenn eine Richtlinie, die diese Einstellung enthält, auf dem Computer wirksam wird.

17.1.1 Gruppen

Im SafeGuard Management Center können auch Computergruppen einem Benutzer (Konto) bzw. Benutzergruppen einem Computer zugewiesen werden.

Beispiel: Service-Konto

Auf diese Weise ist es z. B. einfach möglich, über ein Service-Konto eine große Anzahl Computer zu warten. Dazu müssen sich die Computer in einer Gruppe befinden. Diese Gruppe wird dann einem Service-Konto (Benutzer) zugewiesen. Der Besitzer des Service-Kontos kann sich dann an alle Computer dieser Gruppe anmelden.

Ebenso kann durch das Zuweisen einer Gruppe, die verschiedene Benutzer enthält, diesen Benutzern in einem einfachen Schritt die Anmeldung an einem bestimmten Computer ermöglicht werden.

17.2 Zuweisen von Benutzer- und Computergruppen

So weisen Sie einem Benutzer eine Gruppe von Computern zu:

Hinweis: Das Zuweisen einzelner Benutzer an einen Computer oder umgekehrt, funktioniert analog zur Beschreibung für Gruppen.

1. Klicken Sie auf **Benutzer & Computer**.
2. Zum Zuweisen einer Gruppe von Computern zu einem Benutzer markieren Sie den Benutzer.
3. Klicken Sie im Aktionsbereich auf die Registerkarte **Computer**.

   Unter Verfügbare Computer werden alle Computer und Computergruppen angezeigt.
4. Ziehen Sie die gewünschte Gruppe aus der Liste der verfügbaren Computer in den Aktionsbereich.
5. Ein Dialog, in dem Sie gefragt werden, ob der Benutzer Besitzer aller Computer werden können soll, wird angezeigt.

   Ist für einen Computer im SafeGuard Management Center kein Besitzer festgelegt, wird der erste Benutzer, der sich an diesen Computer anmeldet, automatisch als Besitzer eingetragen. Damit hat er das Recht, anderen Benutzern Zugriff auf diesen Computer zu erlauben. Voraussetzung dafür ist, dass er das Recht „Kann Besitzer werden“ besitzt.

- Beantworten Sie diese Frage mit **Ja**, kann der Benutzer, wenn er sich als erster an diesen Computer anmeldet, Besitzer werden und damit weiteren Benutzern Zugriff gewähren.
- Beantworten Sie diese Frage mit **Nein**, kann der Benutzer nicht Besitzer dieses Computers werden.

  Für ein Service-Konto ist es in der Regel nicht notwendig, dass der Inhaber dieses Kontos Besitzer der Computer werden kann. Diese Einstellung kann nach der initialen Zuweisung geändert werden.

6. Nach der Beantwortung der Frage werden alle Computer aus der zugewiesenen Gruppe im Aktionsbereich angezeigt.

Der Benutzer darf sich jetzt an allen Computern anmelden, die so zugewiesen wurden.

Die Zuweisung einer Benutzergruppe an einen einzelnen Computer funktioniert analog zu dieser Beschreibung.

18 Token und Smartcards

Token und Smartcards sind Hardware-Komponenten, die einen autorisierten Benutzer eines Computersystems bei der Authentisierung unterstützen. Auf ihnen können Zertifikate, digitale Signaturen oder biometrische Daten gespeichert werden. Es können keine Daten manipuliert werden.

Die Authentisierung mit Benutzername und Kennwort genügt heutzutage oft nicht mehr den Kundenanforderungen nach optimalem Schutz vor Angriffen von Dritten. Deswegen bietet SafeGuard Enterprise als Alternative dazu und zur Steigerung der Sicherheit die Anmeldung mit Token und Smartcards. Die Token-Anmeldung basiert auf dem Prinzip der Zwei-Faktor-Authentisierung: Ein Benutzer verfügt über einen Token (Besitz), kann den Token aber nur nutzen, wenn er das spezifische Token-Kennwort kennt (Wissen). Bei Verwendung eines Token oder einer Smartcard benötigen die Benutzer zur Authentisierung nur noch den Token und eine PIN.

Hinweis: Smartcards und Token werden aus Sicht von SafeGuard Enterprise gleich behandelt. Deshalb werden im Produkt und im Handbuch die Begriffe "Token" und "Smartcard" gleichgesetzt.

Token werden unterstützt:

- in der Power-on Authentication
- auf Betriebssystemebene
- zur Anmeldung am Management Center

Wenn ein Token für einen Benutzer ausgestellt wird, werden Daten wie Hersteller, Typ, Seriennummer, Anmeldedaten und Zertifikate in der SafeGuard Enterprise-Datenbank hinterlegt. Token werden hierbei anhand der Seriennummer identifiziert und sind dann in SafeGuard Enterprise bekannt.

Dies bietet wichtige Vorteile:

- Es ist sichtbar, welche Token im Umlauf sind und welchen Benutzern sie zugeordnet sind.
- Es ist klar erkennbar, wann die Token ausgestellt wurden.
- Wenn Token verlorengegangen sind, kann der Sicherheitsbeauftragte sie identifizieren und für die Authentisierung sperren. Damit kann Datenmissbrauch verhindert werden.
- Trotzdem kann der Sicherheitsbeauftragte über Challenge/Response die Anmeldung ohne Token zeitweilig erlauben, z. B. wenn ein Benutzer seine PIN vergessen hat.

18.1 Smartcards

Um eine Smartcard an SafeGuard Enterprise benutzen zu können, wird außer der Smartcard ein Kartenleser sowie auf PC-Seite ein Kartentreiber benötigt. Außerdem setzt die Kommunikation der Smartcards und Kartenleser mit SafeGuard Enterprise bestimmte Middleware in Form eines PKCS#11-Moduls voraus.

18.1.1 Smartcards und Smartcard-Leser/-Treiber

SafeGuard Enterprise unterstützt nicht-kryptographische und kryptographische Anmeldeverfahren bei der Power-on Authentication. Bei nicht-kryptographischen Smartcards werden Benutzerkennung und Kennwort auf der Karte gespeichert. Kryptographische Smartcards verwenden zur Authentisierung RSA-Schlüsselpaare (Zertifikate).

Windows

- Auf Windows-Betriebssystemebene werden PC/SC-kompatible Kartenleser unterstützt. Die PC/SC-Schnittstelle regelt die Kommunikation zwischen PC und Smartcard. Viele dieser Kartenleser sind bereits Teil der Windows-Installation.
- Smartcards benötigen PKCS#11 kompatible Smartcard-Treiber, damit sie von SafeGuard Enterprise unterstützt werden können.

Power-on Authentication

Eine genaue Liste aller unterstützten Smartcards, Smartcard-Leser und -Treiber an der Power-on Authentication finden Sie in den Release Notes.

- An der Power-on Authentication wird die PC/SC-Schnittstelle unterstützt, die die Kommunikation zwischen PC und Smartcard regelt. Die unterstützten Smartcard-Treiber sind fest implementiert und die Benutzer können keine zusätzlichen Treiber hinzufügen. Die passenden Smartcard-Treiber müssen über eine Richtlinie in SafeGuard Enterprise aktiviert werden.
- Die Schnittstelle für Smartcard-Leser ist standardisiert und viele Kartenleser haben eine USB-Schnittstelle oder eine ExpressCard/54-Schnittstelle und implementieren den CCID-Standard. In SafeGuard Enterprise ist dies eine Voraussetzung, um bei der Power-on Authentication unterstützt zu werden. Außerdem muss auf Treiber-Seite das PKCS#11-Modul unterstützt werden.

18.1.2 Unterstützte Smartcards an der Power-on Authentication

SafeGuard Enterprise unterstützt ein große Anzahl von Smartcards und Smartcard-Lesern, sowie gängige Smartcard-Treiber an der Power-on Authentication. An SafeGuard Enterprise werden Token/Smartcards unterstützt, die 2.048 Bit RSA-Operationen unterstützen. Da die Unterstützung von Smartcards von Release zu Release erweitert wird, werden die in der jeweils aktuellen SafeGuard Enterprise Version unterstützten Token und Smartcards in den Release Notes aufgeführt.

18.1.3 Unterstützte Middleware

Die in der folgenden Liste aufgeführte Middleware wird über deren jeweiliges PKCS#11-Modul unterstützt. PKCS#11 ist eine standardisierte Schnittstelle zur Anbindung kryptographischer Token/Smartcards an verschiedenste Software und dient hier der Kommunikation zwischen kryptographischen Token/Smartcard, Smartcard-Leser und SafeGuard Enterprise.

Hersteller	Middleware
ActivIdentity	ActivClient
Aladdin	eToken PKI Client
AET	SafeSign Identity Client
Charismatics	Smart Security Interface
RSA	RSA Authentication Client 2.x RSA Smart Card Middleware 3.x
Siemens	CardOS API
A-Trust	a.sign Client
Gemalto	Gemalto .NET Card Gemalto Classic Client Gemalto Access Client
IT Solution GmbH	IT Solution trustWare CSP+
Sertifitseerimiskeskus AS	Estonian ID Card
T-Systems	NetKey 3.0

Lizenzinformationen für Siemens und Charismatics:

Beachten Sie, dass für die Benutzung der jeweiligen Middleware für das Standard-Betriebssystem eine Lizenzvereinbarung mit Siemens Medical/Charismatics erforderlich ist. Um Lizenzen zu erwerben, wenden Sie sich bitte an:

- Global Siemens Healthcare Headquarters
  Siemens AG
  Healthcare Sector
  Henkestrasse 127
  D-91052 Erlangen
  Tel.: +49 69 797 6602
- *http://www.charismathics.com/cryptoshop/shop_content.php*
  oder
  sales@charismathics.com

Die Middleware wird über eine Richtlinie in SafeGuard Enterprise gesetzt. Das SafeGuard Enterprise Client-Konfigurationspaket muss zudem auf dem PC installiert sein, auf dem das Management Center läuft.

18.2 USB-Token

USB-Token bestehen wie Smartcards aus einem Smartcard-Leser und einer Smartcard, wobei sich die beiden Einheiten in einem Gehäuse befinden.

18.2.1 Unterstützte USB-Token an der Power-on Authentication

SafeGuard Enterprise unterstützt sehr viele USB-Token. Voraussetzung ist, dass eine der von der Power-on Authentication von SafeGuard Enterprise unterstützten Smartcards eingebaut ist und einer der unterstützten Treiber verwendet wird. Außerdem müssen die USB-Token von der entsprechenden Middleware unterstützt werden.

Da die Unterstützung von Token von Release zu Release erweitert wird, werden die in der jeweils aktuellen SafeGuard Enterprise Version unterstützten Token und Smartcards in den Release Notes aufgeführt.

18.3 Mit Token arbeiten

Folgende Aufgaben müssen Sie durchführen, damit Token zur Authentisierung verwendet werden können:

1. Leeren Token initialisieren
2. Token für Benutzer und Sicherheitsbeauftragte ausstellen
3. Zertifikate und Schlüssel auf Token schreiben
4. Richtlinien für Token festlegen

Sie können auch einen bereits mit Daten einer anderen Anwendung versehenen Token zur Authentisierung verwenden, sofern genügend freier Speicherplatz für die Zertifikate und Anmeldeinformationen darauf vorhanden ist.

Folgende Möglichkeiten stehen Ihnen in SafeGuard Enterprise zur komfortablen Verwaltung von Token zur Verfügung:

- Token-Informationen anzeigen und filtern
- PINs initialisieren, ändern, zurücksetzen und sperren
- Token-Daten lesen und löschen
- Token sperren

18.4 Token initialisieren

Bevor ein „leerer“, unformatierter Token in SafeGuard Enterprise für einen Benutzer ausgestellt werden kann, muss er nach den Angaben des Token-Herstellers für die Verwendung vorbereitet, also initialisiert werden. Bei der Initialisierung wird er mit Basisinformationen, z. B. den Standard-PINs, beschrieben. Dies erfolgt über die Initialisierungs-Software des Token-Herstellers.

Für weitere Informationen wenden Sie sich an den entsprechenden Token-Hersteller.

18.4.1 Middleware auf dem Client installieren

Installieren Sie anschließend die korrekte Middleware sowohl auf dem PC, auf dem das SafeGuard Management Center läuft, als auch auf dem entsprechenden Benutzer-Computer, siehe *Unterstützte Middleware* auf Seite 200.

18.4.2 Middleware (PKCS#11-Modul) aktivieren

Bevor Sie den Token ausstellen, müssen Sie ihm im SafeGuard Management Center über eine Richtlinie die passende Middleware in Form des PKCS#11-Moduls zuweisen. Dies müssen Sie sowohl für den Computer, auf dem das SafeGuard Management Center läuft, als auch für den Benutzer-Computer erledigen. Dann erst kann SafeGuard Enterprise mit dem Token kommunizieren. Die Einstellung für das PKCS#11-Modul können Sie folgendermaßen über eine Richtlinie festlegen.

Voraussetzung: Die Middleware wurde auf dem entsprechenden PC installiert und der Token wurde initialisiert. Das SafeGuard Enterprise Client-Konfigurationspaket muss zudem auf dem PC installiert sein, auf dem das Management Center läuft.

Sie befinden sich im geöffneten Management Center im Bereich **Richtlinien**.

1. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
2. Legen Sie eine neue Richtlinie des Typs **Spezifische Computereinstellungen** an oder wählen Sie eine bereits bestehende Richtlinie dieses Typs aus.
3. Wählen Sie im rechten Arbeitsbereich unter **Tokenunterstützung** > **Modulname** die passende Middleware aus. Speichern Sie die Einstellungen.
4. Weisen Sie die Richtlinie zu.

SafeGuard Enterprise kann nun mit dem Token kommunizieren und den Token verwalten. Der Token kann nun ausgestellt werden.

18.5 Token ausstellen

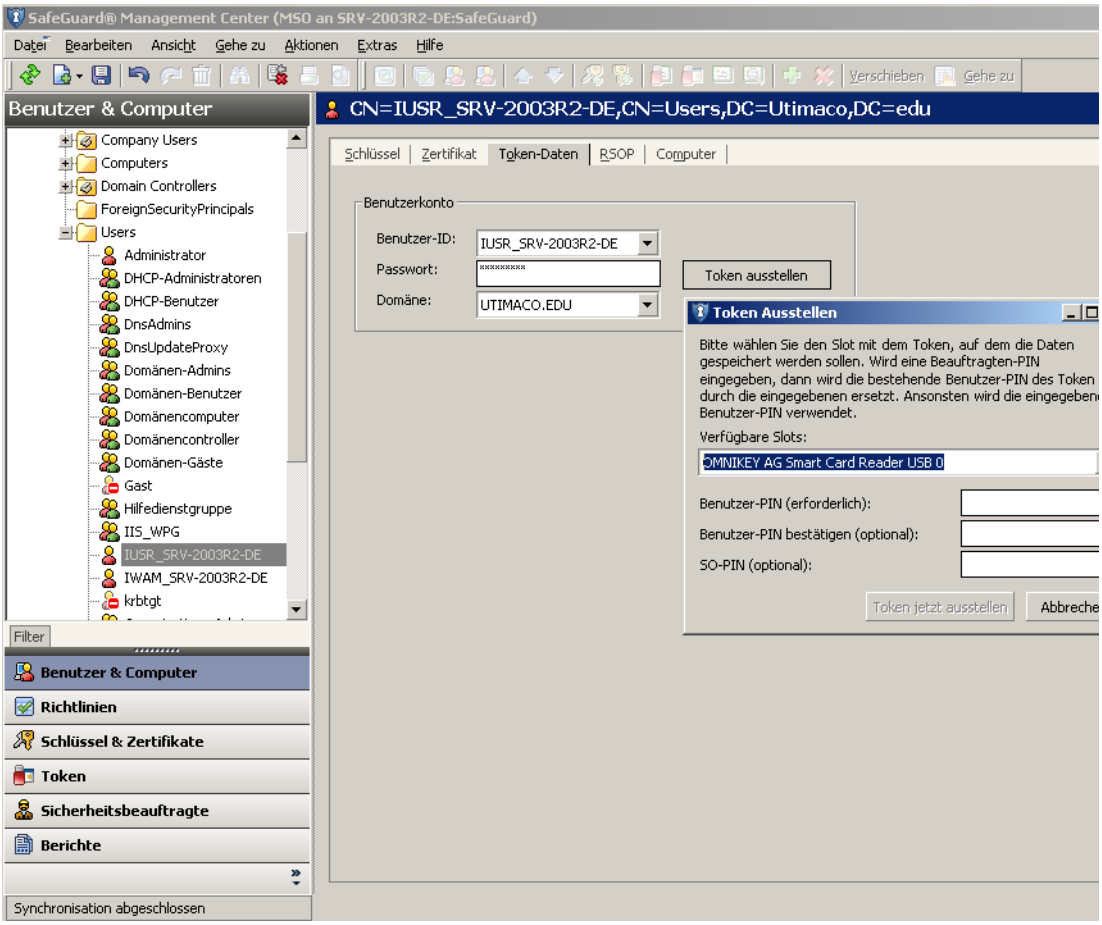
Beim Ausstellen eines Token in SafeGuard Enterprise werden Daten auf den Token geschrieben, die dann für die Authentisierung verwendet werden. Bei den Daten handelt es sich um die Anmeldeinformationen und Zertifikate.

In SafeGuard Enterprise können Token für folgende Benutzerrollen ausgestellt werden:

- Token für normale Benutzer
- Token für Sicherheitsbeauftragte (SO)

Zugriff auf den Token haben sowohl der Benutzer als auch der Sicherheitsbeauftragte (SO). Der Benutzer ist der, der den Token benutzen soll. Nur er hat Zugriff auf private Objekte und Schlüssel.
Der SO hat nur Zugriff auf öffentliche Objekte, kann allerdings die Benutzer-PIN zurücksetzen.

18.5.1 Token oder Smartcard für Benutzer ausstellen



Voraussetzung: Der Token muss initialisiert und das passende PKCS#11-Modul aktiviert worden sein. Das SafeGuard Enterprise Client-Konfigurationspaket muss zudem auf dem PC installiert sein, auf dem das Management Center läuft.

Sie befinden sich im geöffneten Management Center im Bereich **Benutzer & Computer**.

1. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
2. Markieren Sie den Benutzer, für den ein Token ausgestellt werden soll, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Token-Daten**.

3. Gehen Sie im Dialog **Token-Daten** wie folgt vor:

   a) Wählen Sie die Benutzer-ID und Domäne des betreffenden Benutzers aus und geben Sie sein Windows-Kennwort ein.

   b) Klicken Sie auf **Token ausstellen**.

4. Wählen Sie im Dialog **Token ausstellen** den entsprechenden Slot für den Token aus.

5. Vergeben Sie eine neue **Benutzer-PIN** und wiederholen Sie die Eingabe.

6. Geben Sie unter **SO-PIN** die vom Hersteller erhaltene Standard-PUK bzw. die bei der Token-Initialisierung vergebene PIN ein.

Hinweis: Wenn Sie nur das Feld **Benutzer-PIN (erforderlich)** ausfüllen, muss die Benutzer-PIN mit der PIN übereinstimmen, die bei der Token-Initialisierung vergeben wurde. Sie müssen die Benutzer-PIN dann nicht wiederholen und keine SO-PIN eingeben.

7. Klicken Sie auf **Token jetzt ausstellen**.

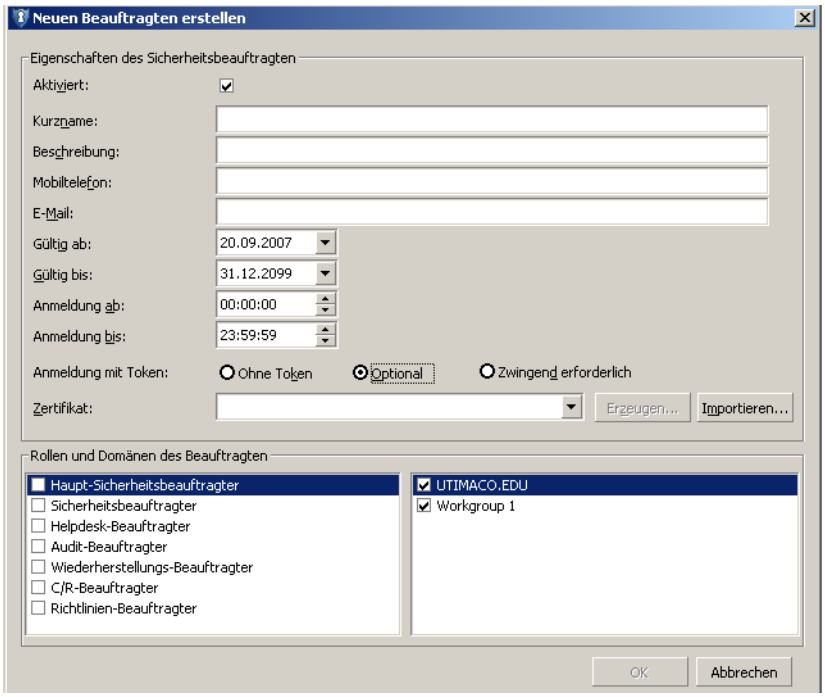
Der Token wird ausgestellt, die Anmeldeinformationen auf den Token geschrieben und die Token-Informationen in der SafeGuard Enterprise-Datenbank hinterlegt. Im Bereich **Token** können Sie sich in der Registerkarte **Token-Information** die Daten anzeigen lassen.

18.5.2 Token oder Smartcard für Sicherheitsbeauftragte ausstellen

Bei der Erstinstallation von SafeGuard Enterprise besteht für den ersten Sicherheitsbeauftragten (SO) bereits die Möglichkeit, sich einen Token ausstellen zu lassen und den Anmeldemodus festzulegen (siehe Installationshandbuch). Für alle weiteren Sicherheitsbeauftragten nehmen Sie die Ausstellung eines Token im SafeGuard Management Center vor.

Voraussetzung: Der Token muss initialisiert sein und das passende PKCS#11-Modul aktiviert worden sein. Sie benötigen die Rechte, die Angaben für den SO festlegen zu dürfen.

Sie befinden sich im geöffneten Management Center im Bereich **Sicherheitsbeauftragte**.



1. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
2. Markieren Sie im linken Navigationsfenster **Sicherheitsbeauftragte** und wählen Sie im Kontextmenü **Neu** > **Neuer Beauftragter**.
3. Wenn sich der SO wahlweise mit oder ohne Token authentisieren soll, aktivieren Sie im rechten Arbeitsbereich bei **Anmeldung mit Token** die Einstellung **Optional**.
4. Wenn sich der SO ausschließlich mit dem Token authentisieren soll, aktivieren Sie bei **Anmeldung mit Token** die Einstellung **Zwingend erforderlich**. Bei dieser Einstellung verbleibt der private Schlüssel auf dem Token. Der Token muss immer eingesteckt sein, ansonsten wird ein Neustart des Systems notwendig.
5. Wenn Sie neue Zertifikate erzeugen wollen, klicken Sie auf **Erzeugen**. Geben Sie das Kennwort für das Zertifikat zweimal ein und bestätigen Sie mit **OK**. Legen Sie den Speicherort für das Zertifikat fest.
6. Wenn Sie Zertifikate importieren wollen, klicken Sie auf **Importieren**. Öffnen Sie die gewünschte Zertifikatedatei. Nach Zertifikaten wird zuerst in einer Zertifikatedatei, dann auf dem Token gesucht. Die Zertifikate können an den jeweiligen Speicherorten verbleiben.
7. Aktivieren Sie die Rollen und Domänen, die dem Beauftragten zugewiesen werden sollen, unter **Rollen und Domänen des Beauftragten**.

8. Bestätigen Sie die Eingaben mit **OK**.

Der SO wird angelegt, der Token wird ausgestellt, die Anmeldedaten werden je nach Einstellung auf den Token geschrieben und die Token-Informationen werden in der SafeGuard Enterprise-Datenbank hinterlegt. Im Bereich **Token** können Sie sich in der Registerkarte **Token-Information** die Daten anzeigen lassen.

18.6 Token oder Smartcards mit Zertifikaten versehen

Außer den Anmeldeinformationen können auf einen Token auch Zertifikate geschrieben werden. Es ist möglich, den privaten Teil des Zertifikats (.p12-Datei) ausschließlich auf dem Token zu speichern. Im Regelfall haben Benutzer dann aber nur noch bei Anmeldung mit dem Token Zugriff auf ihren privaten Schlüssel. Es wird empfohlen, PKI-Zertifikate zu verwenden.

Sie können Authentisierungsdaten auf verschiedene Arten dem Token zuweisen:

- durch Generieren von Zertifikaten direkt auf dem Token
- durch Zuweisen von Daten, die sich bereits auf dem Token befinden
- durch Importieren von Zertifikaten aus einer Datei
- SafeGuard Enterprise kann nur dann mit ablaufenden Zertifikaten umgehen, wenn der alte und neue private Schlüssel auf demselben Token stehen.

Hinweis: Es können keine CA-Zertifikate von einem Token geholt und in der Datenbank oder im Zertifikate-Store abgelegt werden. Wenn CA-Zertifikate verwendet werden sollen (oder müssen), müssen diese Zertifikate auch als Datei vorliegen und nicht nur auf dem Token vorhanden sein. Dies gilt auch für CRLs (Certificate Revocation List).
Außerdem muss die Kombination von CA-Zertifikaten und CRL auf einem Token zusammenpassen, da ansonsten eine Anmeldung an allen betroffenen Benutzer-PCs nicht mehr möglich ist. Überprüfen Sie bitte die Korrektheit von CA und CRL. SafeGuard Enterprise übernimmt diese Überprüfung nicht!

- SafeGuard Enterprise kann nur dann mit ablaufenden Zertifikaten umgehen, wenn der alte und neue private Schlüssel auf demselben Token stehen.

18.6.1 Zertifikate durch Token generieren lassen

Sie können neue Zertifikate direkt durch den Token generieren lassen, wenn zum Beispiel keine Zertifikatsinfrastruktur vorhanden ist.

Hinweis: Wird der private Teil des Zertifikats allein auf den Token geschrieben, hat der Benutzer nur mit dem Token Zugriff auf seinen privaten Schlüssel. Der private Schlüssel befindet sich dann nur noch auf dem Token. Wenn der Token verlorengeht, ist der Zugriff auf den privaten Schlüssel nicht mehr möglich.

Voraussetzung: Der Token ist ausgestellt.

Sie befinden sich im geöffneten Management Center im Bereich **Benutzer & Computer**.

1. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
2. Markieren Sie den Benutzer, für den Sie ein Zertifikat generieren wollen, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Zertifikat**.
3. Klicken Sie auf das Symbol **Neues Zertifikat generieren und Token zuweisen** in der SafeGuard Management Center Symbolleiste. Beachten Sie, dass die Schlüssellänge auf die Tokengröße abgestimmt sein muss.
4. Wählen Sie den Slot aus und geben Sie die Token-PIN ein. Klicken Sie auf **Erzeugen**.

Das Zertifikat wird durch den Token generiert und dem Benutzer zugewiesen.

18.6.2 Zertifikat von Token einem Benutzer zuweisen

Wenn sich bereits Zertifikate auf dem Token befinden, die Sie dem Benutzer zuweisen wollen, gehen Sie wie folgt vor:

Voraussetzung: Der Token ist ausgestellt.

Sie befinden sich im geöffneten Management Center im Bereich **Benutzer & Computer**.

1. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
2. Markieren Sie den Benutzer, dem Sie ein Zertifikat zuweisen wollen, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Zertifikat**.
3. Klicken Sie auf das Symbol **Zertifikat von Token zuweisen** in der SafeGuard Management Center Symbolleiste. Wählen Sie das passende Zertifikat aus der Liste aus und geben Sie die Token-PIN ein.
4. Bestätigen Sie mit **OK**.

Das Zertifikat wird dem Benutzer zugewiesen.

18.6.3 Zertifikat aus einer Datei auf den Token aufbringen

Wenn Sie den privaten Teil des Zertifikats (.p12-Datei) aus einer Datei auf den Token aufbringen wollen, gehen Sie wie folgt vor:

Voraussetzung: Der Token ist ausgestellt.

Sie befinden sich im geöffneten Management Center im Bereich **Token**.

1. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
2. Markieren Sie den Token, auf den Sie den privaten Teil des Zertifikats aufbringen wollen, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Anmeldeinformationen & Zertifikate**.
3. Klicken Sie auf das Symbol **P12 auf Token** in der SafeGuard Management Center Symbolleiste. Wählen Sie die passende Zertifikatedatei aus.
4. Geben Sie die Token-PIN und das Kennwort für die .p12-Datei ein und bestätigen Sie mit **OK**.

Der private Teil des Zertifikats wird auf den Token aufgebracht. Sie müssen diesen nun einem Benutzer zuweisen, siehe *Zertifikat von Token einem Benutzer zuweisen* auf Seite 208.

Hinweis: Wählen Sie für einen Token mit Kerberos-Unterstützung dieses Vorgehen. Das Zertifikat muss von SafeGuard Enterprise erkannt werden und auf den Token aufgebracht werden. Falls bereits ein automatisch generiertes Zertifikat existiert, wird es von dem importierten Zertifikat überschrieben.

18.7 Richtlinien für Token zuweisen

Mit der Zuweisung von Richtlinien können Sie weitere Token-Optionen festlegen.
Sie beziehen sich auf:

- PINs
- Anmeldemodus
- Verhalten, wenn der Status des Token nicht mehr erkannt wird
- Entsperrung des Token
- zu benutzende Middleware (PKCS#11-Modul)

18.8 Mit Token an der Power-on Authentication anmelden

So melden Sie sich mit einem Token an der Power-on Authentication an:

Voraussetzung: Achten Sie bitte darauf, dass die USB-Unterstützung im BIOS aktiviert ist. Die Token-Unterstützung muss initialisiert und der Token muss für Sie ausgestellt sein.

1. Stecken Sie den Token an der USB-Schnittstelle ein.
2. Schalten Sie den PC ein und warten Sie, bis der PC an der Power-on Authentication stoppt.
3. Geben Sie Ihre Token-PIN ein.

Die Anmeldung an SafeGuard Enterprise wird ausgeführt.

Anmeldemodus an der Power-on Authentication

Für Token gibt es zwei verschiedene Anmeldeformen. Eine Kombination der beiden Anmeldeformen ist möglich.

- Anmeldung mit Benutzer-ID/Kennwort
- Anmeldung mit Token

  Wenn Sie sich mit einem Token oder einer Smartcard anmelden, können Sie zwischen einem Token-Anmeldemodus mit nicht-kryptographischem Token oder mit Kerberos-Unterstützung (kryptographisch) wählen. Bei Kerberos-Unterstützung ist kein Challenge/Response-Verfahren möglich, da keine Anmeldeinformationen in der POA vorliegen.

Den Modus legt der Sicherheitsbeauftragte für Benutzer und Computer über eine Richtlinie fest.

18.9 Automatische Anmeldung an der POA mit Default-Token-PIN aktivieren

Eine über eine Richtlinie verteilte Default-Token-PIN ermöglicht die automatische Benutzeranmeldung an der Power-on Authentication. Somit muss nicht jeder einzelne Token separat ausgestellt werden und die Benutzer können sich ohne Benutzerinteraktion automatisch an der Power-on Authentication anmelden.

Wenn bei der Anmeldung ein Token benutzt wird und dem Computer eine Default-PIN zugeordnet ist, wird eine durchgehende Anmeldung an der Power-on Authentication durchgeführt. Der Benutzer muss hier keine PIN eingeben.

Als Sicherheitsbeauftragter können Sie diese spezifische PIN in einer Richtlinie vom Typ **Authentisierung** festlegen und sie verschiedenen Computern oder Computergruppen, z. B. allen Computern eines Standorts, zuordnen.

So aktivieren Sie die automatische Anmeldung mit einer Default-Token-PIN:

1. Klicken Sie im SafeGuard Management Center auf **Richtlinien**.
2. Wählen Sie eine Richtlinie des Typs **Authentisierung**.
3. Wählen Sie unter **Anmeldeoptionen** bei **Anmeldemodus** die Option **Token**.
4. Geben Sie bei **PIN für automatische Anmeldung mit Token** die Default-PIN an, die für die automatische Anmeldung verwendet werden soll. In diesem Fall müssen keine PIN-Regeln beachtet werden.

Hinweis: Diese Einstellung steht nur dann zur Verfügung, wenn Sie als möglichen **Anmeldemodus** die Option **Token** gewählt haben.

5. Wählen Sie bei **Durchgehende Anmeldung an Windows** die Option **Durchgehende Anmeldung deaktivieren**. Wenn Sie diese Einstellung nicht auswählen und eine Default-PIN angeben, können Sie die Richtlinie nicht speichern.

   Wenn Sie die **Durchgehende Anmeldung an Windows** dennoch aktivieren möchten, können Sie eine weitere Richtlinie vom Typ **Authentisierung** mit der aktivierten Option erstellen und sie derselben Computergruppe zuordnen. Im RSOP (Resulting Set of Policies) sind somit beide Richtlinien aktiv.
6. Definieren Sie nach Wunsch weitere Token-Einstellungen.
7. Speichern Sie Ihre Einstellungen und ordnen Sie die Richtlinie den relevanten Computern oder Computergruppen zu.

Wenn die automatische Anmeldung auf dem Benutzer-Computer erfolgreich durchgeführt werden konnte, wird Windows gestartet.

Schlägt die automatische Anmeldung auf dem Benutzer-Computer fehl, so wird der Benutzer an der Power-on Authentication aufgefordert, die Token-PIN einzugeben.

18.10 PIN initialisieren, ändern und sperren

Als Sicherheitsbeauftragter können Sie sowohl die Benutzer-PIN als auch die SO-PIN ändern bzw. die Änderung der Benutzer-PIN erzwingen. Dies wird üblicherweise bei der Erstausstellung eines Token notwendig. Außerdem können Sie PINs initialisieren, d.h. neu vergeben und sperren.

Für Benutzer-Computer können Sie weitere PIN-Optionen über Richtlinien festlegen.

Hinweis: Beachten Sie bei PIN-Änderungen, dass manche Token-Hersteller selbst PIN-Regeln festlegen, die den PIN-Regeln von SafeGuard Enterprise widersprechen können. Möglicherweise können PINs deshalb nicht wie gewünscht geändert werden, auch wenn sie den PIN-Regeln von SafeGuard Enterprise entsprechen. Berücksichtigen Sie daher auf jeden Fall die PIN-Regeln des Token-Herstellers. Diese werden im Management Center im Bereich **Token** unter **Token-Information** angezeigt.

Die Verwaltung der PINs wird im Management Center unter **Token** durchgeführt. Der Token ist eingesteckt und links im Navigationsfenster markiert.

18.10.1 Benutzer-PIN initialisieren

Voraussetzung: Die SO-PIN muss bekannt sein.

1. Wenn Sie die Benutzer-PIN neu vergeben wollen, klicken Sie auf das Symbol **Benutzer-PIN initialisieren** in der SafeGuard Management Center Symbolleiste. Geben Sie die SO-PIN ein.
2. Geben Sie die neue Benutzer-PIN ein, wiederholen Sie die Eingabe und bestätigen Sie mit **OK**.

Die Benutzer-PIN wurde initialisiert.

18.10.2 SO-PIN ändern

Voraussetzung: Die bisherige SO-PIN muss bekannt sein.

1. Wenn Sie die SO-PIN ändern wollen, klicken Sie auf das Symbol **PIN des Beauftragten ändern** in der SafeGuard Management Center Symbolleiste.
2. Geben Sie die alte SO-PIN ein.
3. Geben Sie die neue SO-PIN ein, wiederholen Sie die Eingabe und bestätigen Sie mit **OK**.

Die SO-PIN wurde geändert.

18.10.3 Benutzer-PIN ändern

Voraussetzung: Die Benutzer-PIN muss bekannt sein.

1. Wenn Sie die Benutzer-PIN ändern wollen, klicken Sie auf das Symbol **Benutzer-PIN ändern** in der SafeGuard Management Center Symbolleiste.
2. Geben Sie die alte und die neue Benutzer-PIN ein, wiederholen Sie die neue Benutzer-PIN und bestätigen Sie mit **OK**.

Die Benutzer-PIN wurde geändert. Falls Sie die PIN für einen anderen Benutzer geändert haben, teilen Sie ihm die Änderung mit.

18.10.4 PIN-Änderung erzwingen

Um eine Änderung der PIN zu erzwingen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf das Symbol **PIN-Änderung erzwingen** in der SafeGuard Management Center Symbolleiste.

Wenn sich der Benutzer beim nächsten Mal mit dem Token anmeldet, muss er seine Benutzer-PIN ändern.

18.10.5 PIN-Historie

Die PIN-Historie kann gelöscht werden. Klicken Sie dazu auf das Symbol **PIN-Historie löschen**.

18.11 Token und Smartcards verwalten

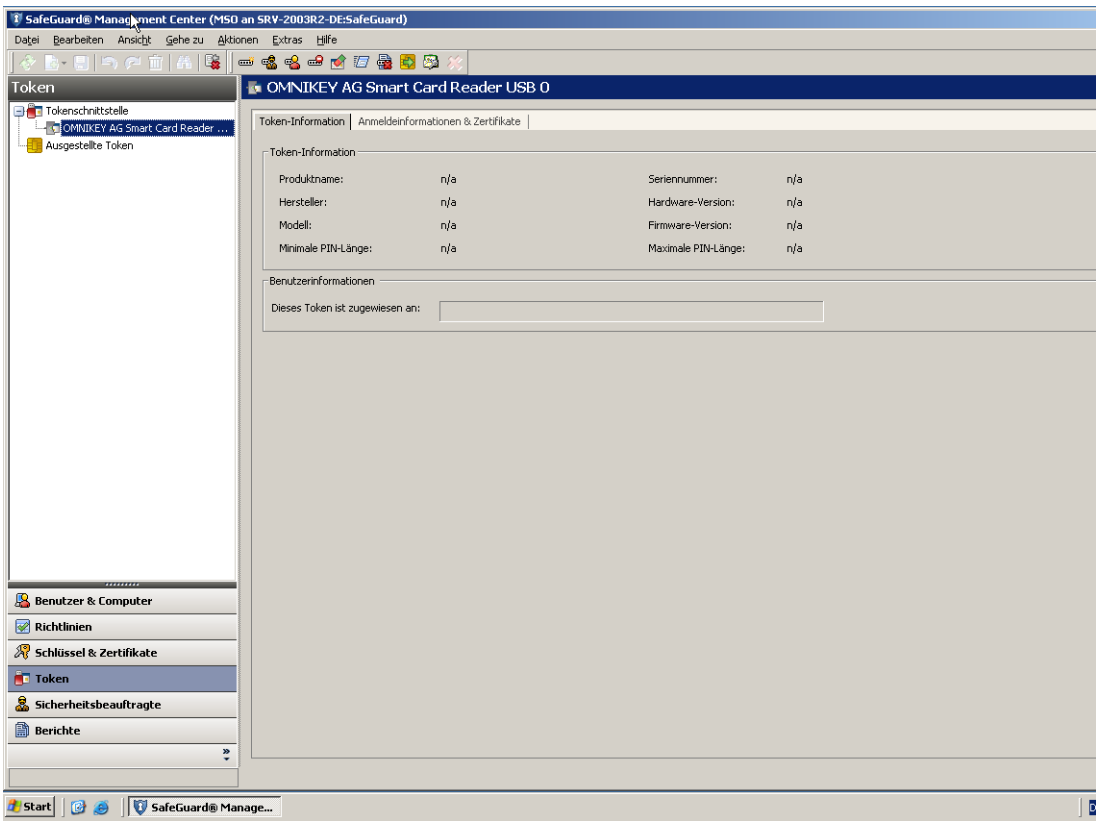
Der Sicherheitsbeauftragte kann sich im Management Center unter **Token** einen Überblick über ausgestellte Token und Zertifikate verschaffen, Übersichten filtern und Token für die Authentisierung sperren oder Daten, die sich auf dem Token befinden, lesen und löschen.

18.11.1 Token/Smartcard-Informationen anzeigen

Als Sicherheitsbeauftragter können Sie sich Informationen über alle oder einzelne ausgestellte Token anzeigen lassen und Übersichten filtern.

Voraussetzung: Der Token muss eingesteckt sein.

Sie befinden sich im geöffneten Management Center im Bereich **Token**.



- Informationen zu einzelnen Token:

  Markieren Sie unter **Token Slots** den gewünschten Token. Unter **Token-Information** werden Hersteller, Typ, Seriennummer, Angaben zu Hardware und PIN-Regeln angezeigt. Außerdem sehen Sie, welchem Benutzer der Token zugeordnet ist.

- Übersicht über Token:

  Markieren Sie **Ausgestellte Token**. Sie können alle ausgestellten Token anzeigen lassen oder die Übersicht nach Benutzern filtern. Es werden die Seriennummer der Token, die Benutzerzuordnung und das Ausstellungsdatum angezeigt. Außerdem erkennen Sie, ob der Token gesperrt ist.

18.11.2 Token/Smartcard-Daten lesen

Als Sicherheitsbeauftragter können Sie mit der für den Token ausgestellten Benutzer-PIN einsehen, welche Daten sich auf dem Token befinden.

Voraussetzung: Der Token muss eingesteckt sein. Die PIN muss dem Sicherheitsbeauftragten bekannt sein. Oder sie muss initialisiert worden sein, siehe *Benutzer-PIN initialisieren* auf Seite 212.

Sie befinden sich im geöffneten Management Center im Bereich **Token**.

1. Markieren Sie links im Navigationsbereich unter **Token Slots** den gewünschten Token und wählen Sie die Registerkarte **Anmeldeinformationen & Zertifikate** aus.
2. Klicken Sie auf das Symbol **Anmeldeinformationen des Benutzers abrufen** und geben Sie die Benutzer-PIN für den Token ein.

Die Daten, die sich auf dem Token befinden, werden angezeigt.

18.11.3 Token/Smartcard-Daten löschen

Als Sicherheitsbeauftragter können Sie die Daten, die über SafeGuard Enterprise auf den Token geschrieben wurden, vom Token entfernen.

Voraussetzung: Der Token muss eingesteckt sein.

Sie befinden sich im geöffneten Management Center im Bereich **Token**.

1. Markieren Sie links im Navigationsbereich unter **Token Slots** den gewünschten Token.
2. Klicken Sie auf das Symbol **Token löschen** in der SafeGuard Management Center Symbolleiste.
3. Geben Sie die dem Token zugeordnete SO-PIN ein und bestätigen Sie mit **OK**.

Es werden alle Daten entfernt, die von SafeGuard Enterprise verwaltet werden. Zertifikate verbleiben auf dem Token.

Die Benutzer-PIN wird auf 1234 zurückgesetzt.

Auf diese Weise gelöschte Token werden automatisch aus der Liste der ausgestellten Token entfernt.

18.11.4 Token oder Smartcard sperren

Als Sicherheitsbeauftragter können Sie Token sperren. Dies ist z. B. sinnvoll, wenn ein Token verloren gegangen ist.

Sie befinden sich im geöffneten Management Center im Bereich **Token**.

1. Markieren Sie links im Navigationsbereich **Ausgestellte Token**.
2. Markieren Sie den Token, der gesperrt werden soll, und klicken Sie auf das Symbol **Token sperren** in der SafeGuard Management Center Symbolleiste.

Der Token wird für die Authentisierung gesperrt, der zugeordnete Benutzer kann sich nicht mehr damit anmelden. Der Token kann nur mithilfe der SO-PIN entsperrt werden.

19 SafeGuard Data Exchange

Mit SafeGuard Data Exchange lassen sich Daten, die auf mit Endpoint-Computern verbundenen Wechselmedien gespeichert werden, verschlüsseln und mit anderen Benutzern austauschen. Alle Ver- und Entschlüsselungsprozesse laufen transparent und mit minimaler Benutzerinteraktion ab.

Nur Benutzer, die über die entsprechenden Schlüssel verfügen, können den Inhalt der verschlüsselten Daten lesen. Alle nachfolgenden Verschlüsselungsprozesse laufen transparent.

In der zentralen Administration definieren Sie, wie Daten auf Wechselmedien behandelt werden sollen.

Als Sicherheitsbeauftragter legen Sie die spezifischen Einstellungen in einer Richtlinie vom Typ **Geräteschutz** mit *Ziel des Geräteschutzes:* **Wechselmedien** fest.

Für SafeGuard Data Exchange muss dateibasierende Verschlüsselung benutzt werden.

Gruppenschlüssel

Für den Austausch von verschlüsselten Daten zwischen Benutzern müssen SafeGuard Enterprise Gruppenschlüssel verwendet werden. Wenn sich der Gruppenschlüssel in den Schlüsselringen der Benutzer befindet, erhalten diese vollen transparenten Zugriff auf die mit ihren Computern verbundenen Wechselmedien.

Auf Computern ohne SafeGuard Enterprise ist der Zugriff auf verschlüsselte Daten auf Wechselmedien nicht möglich. Eine Ausnahme ist hier der zentrale definierte Domänen-/ Gruppenschlüssel, der in Verbindung mit der Medien-Passphrase benutzt werden kann.

Hinweis: Um verschlüsselte Daten auf Wechselmedien auch auf/mit Computern ohne SafeGuard Enterprise zu benutzen/weiterzugeben, können Sie SafeGuard Portable benutzen. Für SafeGuard Portable ist die Verwendung von lokalen Schlüsseln oder einer Medien-Passphrase erforderlich.

Lokale Schlüssel

SafeGuard Data Exchange unterstützt die Verschlüsselung mit lokalen Schlüsseln. Lokale Schlüssel werden auf dem Benutzercomputer erzeugt und können zur Verschlüsselung von Wechselmedien benutzt werden. Die Schlüssel werden durch Eingabe einer Passphrase erstellt. In der SafeGuard Enterprise Datenbank wird jeweils eine Sicherungskopie des lokalen Schlüssels erstellt.

Hinweis: Ein Benutzer ist standardmäßig dazu berechtigt, lokale Schlüssel zu erzeugen. Sollen Benutzer nicht dazu berechtigt sein, so müssen Sie diese Option explizit deaktivieren. Dies muss in einer Richtlinie vom Typ **Geräteschutz** mit *Ziel des Geräteschutzes*: **Lokale Datenträger** erfolgen (**Allgemeine Einstellungen** > **Benutzer darf einen lokalen Schlüssel erzeugen**: Nein).

Werden lokale Schlüssel zum Verschlüsseln von Dateien auf Wechselmedien verwendet, lassen sich diese Dateien auf einem Computer ohne SafeGuard Data Exchange mit SafeGuard Portable entschlüsseln. Beim Öffnen der Dateien mit SafeGuard Portable wird der Benutzer dazu aufgefordert, die Passphrase einzugeben, die beim Erzeugen des Schlüssels angegeben wurde. Wenn dem Benutzer die Passphrase bekannt ist, kann er die Datei öffnen.

Mit SafeGuard Portable erhält jeder Benutzer, der die entsprechende Passphrase kennt, Zugang zu verschlüsselten Dateien auf Wechselmedien. Auf diese Weise ist ein Austausch von verschlüsselten Daten mit Partnern, die nicht über SafeGuard Enterprise verfügen, möglich. Sie benötigen lediglich SafeGuard Portable sowie die Passphrase für die Dateien, auf die sie zugreifen sollen.

Durch Verwendung von verschiedenen lokalen Schlüsseln für die Verschlüsselung von Dateien auf Wechselmedien lässt sich der Zugang zu den Dateien sogar selektiv einschränken. Zum Beispiel: Sie verschlüsseln die Dateien auf einem USB-Stick mit einem Schlüssel mit der Passphrase *my_localkey*. Für eine einzelne Datei mit dem Dateinamen *FürPartner.doc* verwenden Sie die Passphrase *partner_lokalerSchlüssel*. Wenn Sie den USB-Stick nun an einen Partner weitergeben und ihm die Passphrase *partner_lokalerSchlüssel* mitteilen, hat dieser nur Zugriff auf die Datei *FürPartner.doc*.

Hinweis: Standardmäßig wird SafeGuard Portable automatisch auf alle mit dem System verbundenen Wechselmedien kopiert. Um SafeGuard Portable nicht automatisch auf die Wechselmedien zu kopieren, deaktivieren Sie die Option **SafeGuard Portable auf Wechselmedien kopieren** in einer Richtlinie vom Typ **Geräteschutz**.

Medien-Passphrase

SafeGuard Data Exchange ermöglicht es Ihnen auch festzulegen, dass eine einzige Medien-Passphrase für alle Wechselmedien - mit Ausnahme von optischen Medien - auf den Endpoint-Computern erstellt werden muss. Die Medien-Passphrase ermöglicht sowohl den Zugriff auf alle zentral definierten Domänen-/Gruppenschlüssel als auch auf alle in SafeGuard Portable verwendeten lokalen Schlüssel. Der Benutzer muss nur eine einzige Passphrase eingeben und erhält Zugriff auf alle verschlüsselten Dateien in SafeGuard Portable. Dabei spielt es keine Rolle, welcher lokale Schlüssel für die Verschlüsselung verwendet wurde.

Auf jedem Computer wird automatisch ein einzigartiger Medienverschlüsselungsschlüssel für die Datenverschlüsselung für jedes Medium erstellt. Dieser Schlüssel ist durch die Medien-Passphrase und einen zentral definierten Domänen-/Gruppenschlüssel gesichert. Auf einem Computer mit SafeGuard Data Exchange ist es daher nicht notwendig, die Medien-Passphrase einzugeben, um auf die verschlüsselten Dateien auf Wechselmedien zuzugreifen. Der Zugriff wird automatisch gewährt, wenn sich der entsprechende Schlüssel im Schlüsselring des Benutzers befindet.

Der zu verwendende Domänen-/Gruppenschlüssel muss unter **Für Verschlüsselung definierter Schlüssel** festgelegt werden.

Die Medien-Passphrase-Funktionalität steht zur Verfügung, wenn die Option **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen** in einer Richtlinie des Typs **Geräteschutz** aktiviert ist.

Nach dem Wirksamwerden dieser Einstellung auf dem Benutzercomputer wird der Benutzer automatisch aufgefordert, eine Medien-Passphrase einzugeben, wenn er zum ersten Mal Wechselmedien mit dem Computer verbindet. Die Medien-Passphrase ist auf allen Computern, auf denen sich der Benutzer anmelden darf, gültig. Der Benutzer kann die Medien-Passphrase auch ändern. In diesem Fall findet automatisch eine Synchronisierung statt, wenn die Medien-Passphrase auf dem Computer und die Medien-Passphrase der Wechselmedien nicht mehr synchron sind.

Sollte der Benutzer die Medien-Passphrase vergessen, so kann er diese ohne Helpdesk-Unterstützung wiederherstellen.

Hinweis: Um die Medien-Passphrase zu aktivieren, aktivieren Sie die Option **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen** in einer Richtlinie vom Typ **Geräteschutz**.

Medien-Passphrase und Standalone-Computer

Auf einem Standalone-Computer, d. h. Computer, der nicht zentral verwaltet wird, stehen ohne aktvierte Medien-Passphrase-Funktion nach der Installation keine Schlüssel zur Verfügung, da Standalone-Computer nur lokale Schlüssel verwenden. Vor der Benutzung der Verschlüsselung muss der Benutzer einen Schlüssel erzeugen.

Ist die Medien-Passphrase-Funktionalität in einer Wechselmedienrichtlinie für diese Computer aktiviert, so wird der Medienverschlüsselungschlüssel automatisch auf dem Computer erzeugt und kann direkt nach Abschluss der Installation für die Verschlüsselung verwendet werden. Der Schlüssel steht als „vordefinierter“ Schlüssel im Schlüsselring des Benutzers zur Verfügung und wird in Dialogen als `<Benutzername>` für die Schlüsselauswahl angezeigt.

Falls verfügbar, werden die Medienverschlüsselungsschlüssel auch für alle initialen Verschlüsselungsvorgänge verwendet.

19.1 Best Practice

Dieser Abschnitt beschreibt einige typische Anwendungsfälle für SafeGuard Enterprise und deren Umsetzung durch Erstellen der entsprechenden Richtlinien.

Bob und Alice sind zwei Mitarbeiter des gleichen Unternehmens und haben beide SafeGuard Data Exchange installiert. Joe ist ein externer Partner. Auf seinem Computer ist SafeGuard Enterprise nicht installiert.

19.1.1 Unternehmensinterne Anwendung

Bob möchte verschlüsselte Daten auf Wechselmedien an Alice weitergeben. Beide gehören derselben Gruppe an und haben daher den entsprechenden Gruppenschlüssel in ihrem SafeGuard Enterprise Schlüsselring. Da sie den Gruppenschlüssel benutzen, können sie transparent auf die verschlüsselten Dateien zugreifen, ohne eine Passphrase eingeben zu müssen.

Die notwendigen Einstellungen legen Sie in einer Richtlinie vom Typ **Geräteschutz\Wechselmedien** fest:

- **Verschlüsselungsmodus für Medien**: Dateibasierend
- **Schlüssel für die Verschlüsselung**: Definierter Schlüssel aus der Liste
  - Definierter Schlüssel aus der Liste: <Gruppen-/Domänenschlüssel> (z. B. group_users_Bob_Alice@DC=...), um sicherzustellen, dass beide denselben Schlüssel benutzen.

Wenn die Firmenrichtlinien zusätzlich festlegen, dass alle Dateien auf Wechselmedien immer verschlüsselt werden sollen, fügen Sie folgende Einstellungen hinzu:

- **Initialverschlüsselung aller Dateien**: Ja
  Stellt sicher, dass Dateien auf Wechselmedien verschlüsselt werden, sobald die Wechselmedien erstmals mit dem System verbunden werden.
- **Benutzer darf Initialverschlüsselung abbrechen**: Nein
  Der Benutzer kann die Initialverschlüsselung nicht abbrechen, um sie z. B. zu einem späteren Zeitpunkt durchzuführen.
- **Benutzer darf auf unverschlüsselte Dateien zugreifen**: Nein
  Werden auf Wechselmedien unverschlüsselte Dateien entdeckt, so wird der Zugriff auf diese Dateien verweigert.
- **Benutzer darf Dateien entschlüsseln**: Nein
  Der Benutzer darf Dateien auf Wechselmedien nicht entschlüsseln.

- **SafeGuard Portable auf Wechselmedien kopieren**: Nein
  Für die gemeinsame Benutzung von Wechselmedien innerhalb der Arbeitsgruppe ist SafeGuard Portable nicht erforderlich. Außerdem würde SafeGuard Portable das Entschlüsseln von Dateien auf Computern ohne SafeGuard Enterprise erlauben.

Die Benutzer können Daten einfach durch Austausch von Wechselmedien gemeinsam nutzen. Wenn sie die Wechselmedien mit ihren Computern verbinden, haben sie transparenten Zugriff auf verschlüsselte Dateien.

Achtung: Dieser Anwendungsfall kann durch Benutzung von SafeGuard Enterprise Device Encryption umgesetzt werden. Hier ist das gesamte Wechselmedium sektorbasierend verschlüsselt.

19.1.2 Anwendung bei Heimarbeit oder für persönlichen Gebrauch auf Dritt-Computern

Heimarbeit:

Bob möchte seine verschlüsselten Wechselmedien auf seinem Computer zuhause benutzen, auf dem SafeGuard Enterprise nicht installiert ist. Auf seinem Computer zuhause entschlüsselt Bob Dateien mit SafeGuard Portable. Da für alle seine Wechselmedien eine einzige Medien-Passphrase definiert ist, muss Bob nur SafeGuard Portable öffnen und die Medien-Passphrase eingeben. Danach hat Bob transparenten Zugriff auf alle verschlüsselten Dateien, unabhängig davon, welcher Schüssel für die Verschlüsselung verwendet wurde.

Persönlicher Gebrauch auf Dritt-Computern:

Bob verbindet das Wechselmedium mit Joes (externer Partner) Computer und gibt die Medien-Passphrase ein, um Zugriff auf die auf dem Medium gespeicherten verschlüsselten Dateien zu erhalten. Bob kann die Dateien nun - verschlüsselt oder unverschlüsselt - auf Joes Computer kopieren.

Verhalten auf dem Endpoint-Computer

- Bob verbindet das Wechselmedium zum ersten Mal mit dem Computer.
  Der Medienverschlüsselungsschlüssel, der für jedes Medium einzigartig ist, wird automatisch erzeugt.
- Bob wird aufgefordert, die Medien-Passphrase für die Offline-Nutzung über SafeGuard Portable einzugeben.
- Der Benutzer muss nichts über den zu verwendenden Schlüssel oder den Schlüsselring wissen. Der Medienverschlüsselungschlüssel wird ohne Benutzerinteraktion immer für die Datenverschlüsselung verwendet. Der Medienverschlüsselungschlüssel ist für den Benutzer auch nicht sichtbar. Nur der zentral definierte Gruppen-/Domänenschlüssel ist sichtbar.

- Bob und Alice haben innerhalb der gleichen Gruppe oder Domäne transparenten Zugriff, da sie beide den gleichen Gruppen-/Domänenschlüssel verwenden.
- Wenn Bob auf verschlüsselte Dateien auf Wechselmedien auf einem Computer ohne SafeGuard Data Exchange zugreifen möchte, kann er die Medien-Passphrase in SafeGuard Portable benutzen.

Die notwendigen Einstellungen legen Sie in einer Richtlinie vom Typ **Geräteschutz\Wechselmedien** fest:

- **Verschlüsselungsmodus für Medien**: Dateibasierend
- **Schlüssel für die Verschlüsselung**: Definierter Schlüssel aus der Liste
  - **Definierter Schlüssel aus der Liste**: <Gruppen-/Domänenschlüssel> (z. B. group_users_Bob_Alice@DC=...), um sicherzustellen, dass beide denselben Schlüssel benutzen.
- **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen**: Ja
  Der Benutzer definiert eine Medien-Passphrase auf seinem Computer, die für alle seine Wechselmedien gilt.
- **SafeGuard Portable auf Wechselmedien kopieren**: Ja
  SafeGuard Portable gibt dem Benutzer in einem System ohne SafeGuard Data Exchange Zugriff auf alle verschlüsselten Dateien auf den Wechselmedien durch die Eingabe einer einzigen Medien-Passphrase.

Wenn die Firmenrichtlinien zusätzlich festlegen, dass alle Dateien auf Wechselmedien immer verschlüsselt werden sollen, fügen Sie folgende Einstellungen hinzu:

- **Initialverschlüsselung aller Dateien**: Ja
  Stellt sicher, dass Dateien auf Wechselmedien verschlüsselt werden, sobald die Wechselmedien zum ersten Mal mit dem System verbunden werden.
- **Benutzer darf Initialverschlüsselung abbrechen**: Nein
  Der Benutzer kann die Initialverschlüsselung nicht abbrechen, um sie z. B. zu einem späteren Zeitpunkt durchzuführen.
- **Benutzer darf auf unverschlüsselte Dateien zugreifen**: Nein
  Werden auf Wechselmedien unverschlüsselte Dateien entdeckt, so wird der Zugriff auf diese Dateien verweigert.
- **Benutzer darf Dateien entschlüsseln**: Nein
  Der Benutzer darf Dateien auf Wechselmedien nicht entschlüsseln.

Im Büro haben sowohl Bob als auch Alice transparenten Zugriff auf verschlüsselte Dateien auf Wechselmedien. Zuhause oder auf Dritt-Computern können sie verschlüsselte Dateien mit SafeGuard Portable öffnen. Die Benutzer müssen nur die Medien-Passphrase eingeben und erhalten somit Zugriff auf alle verschlüsselten Dateien. Dies ist eine einfache und sichere Methode für die Verschlüsselung von Daten auf allen Wechselmedien. Ziel dieser Konfiguration ist es, die Benutzerinteraktion auf ein Minimum zu reduzieren und trotzdem jede Datei auf Wechselmedien zu verschlüsseln und den Benutzern Zugriff auf die verschlüsselten Dateien im Offline-Modus zu geben. Der Benutzer darf Dateien auf Wechselmedien nicht entschlüsseln.

Achtung: In dieser Konfiguration sind Benutzer nicht dazu berechtigt, lokale Schlüssel zu erzeugen, da dies in diesem Anwendungsfall nicht notwendig ist. Dies muss in einer Richtlinie vom Typ **Geräteschutz** mit Ziel des Geräteschutzes: **Lokale Datenträger** festgelegt werden (**Allgemeine Einstellungen** > **Benutzer darf einen lokalen Schlüssel erzeugen**: Nein).

- **SafeGuard Portable auf Wechselmedien kopieren**: Nein
  Für die gemeinsame Benutzung von Wechselmedien innerhalb der Arbeitsgruppe ist SafeGuard Portable nicht erforderlich. Außerdem würde SafeGuard Portable das Entschlüsseln von Dateien auf Computern ohne SafeGuard Enterprise erlauben.

Im Büro haben die Benutzer transparenten Zugriff auf verschlüsselte Dateien auf Wechselmedien. Zuhause öffnen sie verschlüsselte Dateien mit SafeGuard Portable. Die Benutzer müssen nur die Medien-Passphrase eingeben und erhalten somit Zugriff auf alle verschlüsselten Dateien, unabhängig davon, welcher Schlüssel für die Verschlüsselung verwendet wurde.

19.1.3 Weitergabe von Wechselmedien an externe Partner

Bob möchte ein verschlüsseltes Medium an Joe (externer Partner) weitergeben, der SafeGuard Data Exchange nicht installiert hat und daher SafeGuard Portable verwenden muss. Bob möchte Joe jedoch nicht auf alle verschlüsselten Dateien auf dem Wechselmedium Zugriff geben. Er kann hierzu einen lokalen Schlüssel erzeugen und die Dateien mit dem lokalen Schlüssel verschlüsseln. Joe kann nun mit SafeGuard Portable die verschlüsselten Dateien mit der Passphrase des lokalen Schlüssels öffnen. Bob dagegen kann immer noch die Medien-Passphrase für den Zugriff auf alle Dateien auf dem Wechselmedium benutzen.

Verhalten auf dem Computer

- Bob verbindet das Wechselmedium zum ersten Mal mit dem Computer.
  Der Medienverschlüsselungsschlüssel, der für jedes Medium einzigartig ist, wird automatisch erzeugt.
- Bob wird aufgefordert, die Medien-Passphrase für die Offline-Nutzung einzugeben.
- Der Medienverschlüsselungsschlüssel wird ohne Benutzerinteraktion für die Datenverschlüsselung verwendet, aber...

- Bob kann nun einen lokalen Schlüssel (z. B. mit der Bezeichnung JoeSchlüssel) für die Verschlüsselung der spezifischen Dateien, die mit Joe ausgetauscht werden sollen, erzeugen oder auswählen.
- Bob und Alice haben innerhalb der gleichen Gruppe oder Domäne transparenten Zugriff, da sie beide den gleichen Gruppen-/Domänenschlüssel verwenden.
- Wenn Bob auf verschlüsselte Dateien auf Wechselmedien auf einem Computer ohne SafeGuard Data Exchange zugreifen möchte, kann er die Medien-Passphrase in SafeGuard Portable benutzen.
- Joe kann auf die spezifischen Dateien durch Eingabe der Passphrase des Schlüssels JoeSchlüssel zugreifen, ohne auf die restlichen Dateien auf dem Wechselmedium zugreifen zu müssen.

Die notwendigen Einstellungen legen Sie in einer Richtlinie vom Typ **Geräteschutz\Wechselmedien** fest:

- **Verschlüsselungsmodus für Medien**: Dateibasierend
- **Schlüssel für die Verschlüsselung**: Beliebiger Schlüssel im Schlüsselring des Benutzers
  Ermöglicht dem Benutzer die Auswahl unterschiedlicher Schlüssel für die Verschlüsselung von Dateien auf Wechselmedien.
  - **Definierter Schlüssel aus der Liste**: <Gruppen-/Domänenschlüssel> (z. B. group_users_Bob_Alice@DC=...), um sicherzustellen, dass beide denselben Schlüssel benutzen und um beiden den transparenten Zugriff auf Wechselmedien zu ermöglichen, wenn sie sie mit ihren Computern im Büro verbinden.
- **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen**: Ja
  Der Benutzer definiert eine Medien-Passphrase auf seinem Computer, die für alle seine Wechselmedien gilt.
- **SafeGuard Portable auf Wechselmedien kopieren**: Ja
  SafeGuard Portable gibt dem Benutzer in einem System ohne SafeGuard Data Exchange Zugriff auf alle verschlüsselten Dateien auf den Wechselmedien durch die Eingabe einer einzigen Medien-Passphrase.

Wenn die Firmenrichtlinien zusätzlich festlegen, dass alle Dateien auf Wechselmedien immer verschlüsselt werden sollen, fügen Sie folgende Einstellungen hinzu:

- **Initialverschlüsselung aller Dateien**: Ja
  Stellt sicher, dass Dateien auf Wechselmedien verschlüsselt werden, sobald die Wechselmedien erstmals mit dem System verbunden werden.
- **Benutzer darf Initialverschlüsselung abbrechen**: Nein
  Der Benutzer kann die Initialverschlüsselung nicht abbrechen, um sie z. B. zu einem späteren Zeitpunkt durchzuführen.

- **Benutzer darf auf unverschlüsselte Dateien zugreifen**: Nein
  Werden auf Wechselmedien unverschlüsselte Dateien entdeckt, so wird der Zugriff auf diese Dateien verweigert.
- **Benutzer darf Dateien entschlüsseln**: Nein

Im Büro haben Bob und Alice transparenten Zugriff auf verschlüsselte Dateien auf Wechselmedien. Zuhause können sie verschlüsselte Dateien mit SafeGuard Portable durch Eingabe der Medien-Passphrase öffnen. Wenn Bob oder Alice die Wechselmedien an einen Dritt-PC weitergeben möchten, auf dem SafeGuard Data Exchange nicht installiert ist, können sie mit lokalen Schlüsseln sicherstellen, dass externe Partner nur auf einige spezifische Dateien zugreifen können. Dies ist eine erweiterte Konfiguration, die durch die Möglichkeit, lokale Schlüssel auf den Computern zu erzeugen, ein höheres Maß an Benutzerinteraktion umfasst.

Achtung: Voraussetzung für diesen Beispielanwendungsfall ist es, dass der Benutzer dazu berechtigt ist, lokale Schlüssel zu erzeugen (Standardeinstellung in SafeGuard Enterprise).

20 Die Power-on Authentication (POA)

SafeGuard Enterprise identifiziert den Benutzer bereits, bevor das Betriebssystem startet. Hierbei startet vorher ein SafeGuard Enterprise eigener Systemkern, der gegen Modifikationen geschützt und versteckt auf der Festplatte gespeichert ist. Erst wenn sich der Benutzer in der POA korrekt authentisiert hat, wird das eigentliche Betriebssystem (Windows) von der verschlüsselten Partition gestartet und der Benutzer später automatisch an Windows angemeldet. Analog wird verfahren, wenn der Computer aus dem Ruhezustand (Hibernation (Suspend to Disk)) wieder eingeschaltet wird.

Die SafeGuard Enterprise Power-on Authentication bietet unter anderem folgende Vorteile:

- Grafische Benutzeroberfläche, mit Mausunterstützung und verschiebbaren Fenstern, und damit einfache, übersichtliche Bedienung.
- Vom Firmenkunden per Richtlinie anpassbares grafisches Layout (Hintergrundbild, Anmeldebild, Willkommensmeldung etc.).
- Unterstützung für eine Reihe von Smartcard-Lesegeräten und Smartcards.
- Unterstützung von Windows-Benutzerkonten und Kennwörtern bereits zum Pre-Boot Zeitpunkt, keine separaten Zugangsdaten mehr, die sich der Benutzer merken muss.
- Unterstützung von Unicode und damit auch fremdsprachigen Kennwörtern bzw. Benutzeroberflächen.

20.1 Ablauf der Anmeldung

SafeGuard Enterprise arbeitet mit zertifikatsbasierter Anmeldung. Deswegen benötigt ein Benutzer zur erfolgreichen Anmeldung in der Power-on Authentication Schlüssel und Zertifikate. Benutzerspezifische Schlüssel und Zertifikate werden jedoch erst nach einer erfolgreichen Windows-Anmeldung erzeugt. Das heißt, nur Benutzer, die sich erfolgreich an Windows angemeldet haben, können sich später auch in der Power-on Authentication authentisieren.

Um den Ablauf der Anmeldung eines Benutzers in SafeGuard Enterprise zu verdeutlichen, im Folgenden eine kurze Einführung. Eine detaillierte Beschreibung der POA-Anmeldevorgänge finden Sie in der SafeGuard Enterprise Benutzerhilfe.

Hinweis: Unter Windows Vista müssen Benutzer erst die Tastenkombination **Strg+Alt+Entf** drücken, um Autologon und Anmeldung zu starten. Diese Einstellung kann der Administrator in der MMC-Konsole im Gruppenrichtlinien-Objekteditor unter **Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen deaktivieren** (Interaktive Anmeldung: kein **Strg+Alt+Entf** erforderlich).

20.1.1 SafeGuard Autologon

Nach dem Neustart erscheint bei der ersten Anmeldung am Endpoint-Computer der SafeGuard Enterprise Autologon.

Was passiert?

1. Ein Autouser wird angemeldet.
2. Der Computer registriert sich automatisch am SafeGuard Enterprise Server.
3. Der Maschinenschlüssel wird an den SafeGuard Enterprise Server geschickt und in der SafeGuard Enterprise Datenbank abgelegt.
4. Maschinenrichtlinien werden an den Endpoint-Computer geschickt.

20.1.2 Windows-Anmeldung

Der Windows-Anmeldedialog erscheint. Der Benutzer meldet sich an.

Was passiert?

1. Benutzer-ID und das verschlüsselte Kennwort werden an den Server geschickt.
2. Benutzerrichtlinien, Zertifikate und Schlüssel werden erzeugt und an den Endpoint-Computer geschickt.
3. Die POA wird aktiviert.

20.1.3 POA-Anmeldung

Nach dem Neustart des Endpoint-Computers erscheint die POA.

Was passiert?

1. Zertifikate und Schlüssel für den Benutzer sind vorhanden, und er kann sich in der POA anmelden.
2. Alle Daten sind sicher mit dem öffentlichen RSA Schlüssel des Benutzers verschlüsselt.
3. Alle weiteren Benutzer, die sich anmelden wollen, müssen erst in die POA importiert werden.

20.1.4 Anmeldeverzögerung

Auf einem durch SafeGuard Enterprise geschützten Computer tritt eine Anmeldeverzögerung in Kraft, wenn ein Benutzer während der Anmeldung an Windows oder an die Power-on Authentication falsche Anmeldeinformationen eingibt. Mit jedem fehlgeschlagenen Anmeldeversuch verlängert sich jeweils die Anmeldeverzögerung. Nach einer fehlgeschlagenen Anmeldung erscheint ein Dialog, der die verbleibende Verzögerungszeit anzeigt.

Hinweis: Wenn ein Benutzer während der Anmeldung mit Token eine falsche PIN eingibt, tritt keine Anmeldeverzögerung ein.

Sie können die Anzahl an erlaubten Anmeldeversuchen in einer Richtlinie vom Typ **Authentisierung** über die Option **Maximalanzahl von erfolglosen Anmeldeversuchen** festlegen.

20.1.5 Computersperre

In einer Richtlinie vom Typ **Authentisierung** können Sie außerdem festlegen, dass der Computer nach der eingestellten Anzahl an fehlgeschlagenen Anmeldeversuchen gesperrt wird. Wählen Sie hierzu bei der Option **Computer sperren** die Einstellung **Ja**. Um eine Computersperre aufzuheben, kann der Benutzer ein Challenge/Response-Verfahren starten.

20.2 Weitere Benutzer importieren

Der erste Benutzer, der sich in Windows anmeldet, ist automatisch in der POA registriert. Zunächst kann sich kein weiterer Windows-Benutzer in der POA anmelden.

Weitere Benutzer müssen mit Hilfe des ersten Benutzers importiert werden. Eine detaillierte Beschreibung zum Importieren weiterer Benutzer finden Sie in der SafeGuard Enterprise Benutzerhilfe.

Eine Richtlinieneinstellung legt fest, wer einen neuen Benutzer importieren darf. Sie finden diese Richtlinie im Management Center unter

Richtlinien

- Typ: Spezifische Computereinstellungen
- Feld: Importieren von neuen Benutzern erlaubt für

Standardeinstellung: Besitzer

Wer der Besitzer eines Endpoint-Computers ist, wird im Management Center festgelegt unter

Benutzer & Computer

- <Computer-Name> markieren
- Registerkarte Benutzer

Hinweis: Für Computer, die im Standalone-Modus laufen, bietet SafeGuard Enterprise POA Access Accounts. POA Access Accounts sind vordefinierte lokale Benutzerkonten, die es Benutzern (z. B. Mitgliedern des IT-Teams) ermöglichen, sich nach der Aktivierung der POA an Endpoint-Computern zur Ausführung administrativer Aufgaben anzumelden. POA Access Accounts ermöglichen die Anmeldung an der POA, eine automatische Anmeldung an Windows erfolgt nicht. Diese Benutzerkonten werden im Bereich **Benutzer & Computer** des SafeGuard Management Center definiert (Benutzer-ID und Kennwort) und werden den Endpoint-Computer über POA-Gruppen in Konfigurationspaketen zugewiesen.

Hinweis: Für detaillierte Informationen zu POA Access Accounts, siehe *POA Access Accounts für die POA-Anmeldung an Standalone-Computern*, Seite 4

20.3 Power-on Authentication konfigurieren

Der POA-Dialog besteht aus folgenden Komponenten:

- Anmeldebild
- Dialogtexte
- Sprache des Tastaturlayouts

Das Erscheinungsbild des POA-Dialogs können Sie u. a. über Richtlinieneinstellungen im SafeGuard Management Center an Ihre jeweiligen Anforderungen anpassen.

20.3.1 Hintergrund- und Anmeldebild

In der Standardeinstellung werden Bilder im SafeGuard-Design als Hintergrund- und Anmeldebild angezeigt. Es ist jedoch möglich, andere Bilder anzuzeigen, z. B. das Firmenlogo.

Hintergrund- und Anmeldebilder werden über eine Richtlinie vom Typ **Allgemeine Einstellungen** festgelegt.

Hintergrund- und Anmeldebilder müssen bestimmten Anforderungen entsprechen, damit sie in SafeGuard Enterprise verwendet werden können:

Hintergrundbild in der POA

Maximale Dateigröße für alle Hintergrundbilder: **500 KB**

SafeGuard Enterprise unterstützt für Hintergrundbilder zwei Varianten:

- **1024x768** (VESA-Modus)

  Farben: keine Einschränkung

  Option im Richtlinientyp **Allgemeine Einstellungen: Hintergrundbild in der POA**

- **640x480** (VGA-Modus)

  Farben: 16

  Option im Richtlinientyp **Allgemeine Einstellungen: Hintergrundbild in der POA (niedrige Auflösung)**

Anmeldebild in der POA

Maximale Dateigröße für alle Anmeldebilder: **100 KB**

SafeGuard Enterprise unterstützt für Anmeldebilder zwei Varianten:

- **413x140**

  Farben: keine Einschränkung

  Option im Richtlinientyp **Allgemeine Einstellungen: Anmeldebild in der POA**

- **413x140**

  Farben: 16

  Option im Richtlinientyp **Allgemeine Einstellungen: Anmeldebild in der POA (niedrige Auflösung)**

Bilder, Informationstexte und Listen müssen zunächst als Dateien (BMP, PNG, JPG oder Textdateien) erstellt werden und können dann im Navigationsbereich registriert werden.

20.3.1.1 Bilder registrieren

So registrieren Sie Bilder:

1. Klicken Sie im **Richtlinien** Navigationsbereich mit der rechten Maustaste auf **Bilder** und wählen Sie **Neu > Bild**.
2. Geben Sie unter **Bildname** einen Namen für das Bild ein.

3. Wählen Sie über die Schaltfläche **[...]** das zuvor erstellte Bild aus.
4. Klicken Sie auf **OK**.

Das neue Bild wird als Unterknoten des Eintrags **Bilder** im Richtlinien-Navigationsbereich angezeigt. Ist ein Bild markiert, wird es im Aktionsbereich angezeigt. Das Bild kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Sie können so weitere Bilder registrieren. Alle registrierten Bilder werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Bild ändern** können Sie das zugeordnete Bild austauschen. Es wird ein Dialog geöffnet, in dem ein anderes Bild ausgewählt werden kann.

20.3.2 Benutzerdefinierter Informationstext in der POA

Sie können die POA für die Anzeige der folgenden **benutzerdefinierten Informationstexte** anpassen:

- Informationstexte, die beim Starten eines Challenge/Response-Verfahrens für Recovery-Vorgänge angezeigt werden (z. B.: "Bitte wenden Sie sich an den Helpdesk unter der Telefonnummer 01234-56789.")

  Option im Richtlinientyp **Allgemeine Einstellungen: Informationstext**

- Rechtliche Hinweise, die nach der Anmeldung an der POA angezeigt werden.

  Option im Richtlinientyp **Spezifische Computereinstellungen: Text für rechtliche Hinweise**

- Text mit zusätzlichen Informationen, der nach der Anmeldung an der POA angezeigt werden soll.

  Option im Richtlinientyp **Spezifische Computereinstellungen: Text für zusätzliche Informationen**

20.3.2.1 Informationstexte registrieren

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Informationstexte beträgt **50 KB**. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden Sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Konvertierung durchgeführt wird, werden Sie durch eine Meldung darüber informiert.

So registrieren Sie die Textdateien:

1. Klicken Sie im **Richtlinien** Navigationsbereich mit der rechten Maustaste auf **Informationstext** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzuzeigenden Text ein.
3. Wählen Sie über die Schaltfläche **[...]** die zuvor erstellte Textdatei aus. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Informationstext im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Sie können weitere Textelemente registrieren. Alle registrierten Textelemente werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Es wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

20.3.3 Sprache der POA-Dialogtexte

Alle Texte in der POA werden nach der Installation der SafeGuard Enterprise Verschlüsselungs-Software mit den Standardeinstellungen in der Sprache angezeigt, die bei der Installation von SafeGuard Enterprise in den Regions- und Sprachoptionen von Windows als Standardsprache am Endpoint-Computer gesetzt ist.

Nach der Installation kann die Sprache in der POA nur über eine im SafeGuard Management Center angelegte Richtlinie geändert werden. Das Ändern der Standardsprache unter Windows, bewirkt keine Änderung der Sprache in der POA.

Die Sprache in der POA wird über eine Richtlinie vom Typ **Allgemeine Einstellungen** (Option **Sprache am Client**) festgelegt.

20.3.4 Tastaturlayout

Beinahe jedes Land besitzt ein eigenes Tastaturlayout, d. h. die Tastenbelegung ist unterschiedlich. Bemerkbar macht sich das Tastaturlayout in der POA bei der Eingabe von Benutzernamen, Kennwort und Response Code.

SafeGuard Enterprise übernimmt als Standard das Tastaturlayout in die POA, das zum Zeitpunkt der Installation in den Regions- und Sprachoptionen von Windows gesetzt ist. Ist unter Windows „Deutsch“ als Tastaturlayout gesetzt, wird in der POA das deutsche Tastaturlayout verwendet.

Die Sprache des verwendeten Tastaturlayouts wird in der POA angezeigt, z. B. „EN“ für Englisch. Neben dem Standard-Tastaturlayout kann das US-Tastaturlayout (Englisch) gewählt werden.

Es gibt bestimmte Ausnahmefälle:

- Das Tastaturlayout wird zwar unterstützt, aufgrund fehlender Schriften (z. B. bei Bulgarisch) werden im Feld **Benutzername** aber nur Sonderzeichen angezeigt.
- Es ist kein spezielles Tastaturlayout verfügbar (z. B. Dominikanische Republik). In solchen Fällen greift die POA auf das Original-Tastaturlayout zurück. Für die Dominikanische Republik ist dies „Spanisch“.

Hinweis: Alle nicht unterstützten Tastaturlayouts verwenden als Standard das US-Tastaturlayout. Das bedeutet, dass auch nur Zeichen erkannt und eingegeben werden können, die im US-Tastaturlayout unterstützt werden. Benutzer können sich demnach nur an der POA anmelden, wenn ihre Benutzernamen und Kennwörter sich aus Zeichen zusammensetzen, die vom US-Tastaturlayout oder dem entsprechenden Original-Layout unterstützt werden.

20.3.4.1 Virtuelle Tastatur

SafeGuard Enterprise bietet die Möglichkeit, in der POA eine virtuelle Tastatur anzeigen zu lassen. Der Benutzer kann dann z. B. Anmeldeinformationen durch Klick auf die am Bildschirm angezeigten Tasten eingeben.

Als Sicherheitsbeauftragter können Sie die Anzeige der virtuellen Tastatur in einer Richtlinie vom Typ **Spezifische Computereinstellungen** über die Option **Virtuelle Tastatur** aktivieren/deaktivieren.

Für die virtuelle Tastatur werden verschiedene Layouts angeboten und das Layout kann mit den gleichen Einstellungen wie das normale Tastaturlayout geändert werden.

20.3.4.2 Tastaturlayout ändern

Das normale wie das virtuelle Tastaturlayout der Power-on Authentication kann nachträglich geändert werden.

So ändern Sie die Sprache des Tastaturlayouts:

1. Wählen Sie **Start > Systemsteuerung > Regions- und Sprachoptionen**.
2. Wählen Sie auf der Registerkarte **Regionale Einstellungen** die gewünschte Sprache aus.
3. Aktivieren Sie dann auf der Registerkarte **Erweitert** unter **Standardeinstellungen für Benutzerkonten** die Option **Alle Einstellungen auf das aktuelle Benutzerkonto und Standardbenutzerprofil anwenden**.
4. Bestätigen Sie die vorgenommenen Einstellungen mit **OK**.

Die POA merkt sich das bei der letzten erfolgreichen Anmeldung verwendete Tastaturlayout und aktiviert dieses beim nächsten Anmelden automatisch. Wenn dieses gemerkte Tastaturlayout über die **Regions- und Sprachoptionen** abgewählt wird, bleibt es dem Anwender noch so lange erhalten, bis er eine andere Sprache ausgewählt hat.

Hinweis: Darüber hinaus ist es erforderlich, die Sprache des Tastaturlayouts für nicht-Unicode-Programme zu ändern.

Falls die gewünschte Sprache nicht im System vorhanden ist, werden Sie von Windows evtl. aufgefordert, die Sprache zu installieren. Danach müssen Sie den Endpoint-Computer zweimal neu starten, damit das neue Tastaturlayout von der Power-on Authentication eingelesen werden und dann auch über diese eingestellt werden kann.

Sie können das gewünschte Tastaturlayout der Power-on Authentication mit der Maus oder mit der Tastatur (**Alt+Shift**) ändern.

Sie können über Start > Ausführen > regedit > HKEY_USERS\.DEFAULT\Keyboard Layout\Preload einsehen, welche Sprachen auf dem System installiert und damit verfügbar sind.

20.4 In der Power-on Authentication unterstützte Hotkeys

Bestimmte Hardware-Einstellungen und -Funktionalitäten können Probleme beim Booten des Endpoint-Computers verursachen, die dazu führen, dass der Rechner im Startvorgang hängen bleibt. Die Power-on Authentication unterstützt eine Reihe von Hotkeys, mit denen sich Hardware-Einstellungen modifizieren und Funktionalitäten modifizieren lassen. Darüber hinaus sind in die auf dem Computer zu installierenden .MSI-Datei Grey Lists und Black Lists integriert, die Funktionen abdecken, von denen ein solches Problemverhalten bekannt ist.

Wir empfehlen, vor jeder größer angelegten SafeGuard Enterprise Installation die aktuelle Version der POA-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht unter ftp://POACFG:POACFG@ftp.ou.utimaco.de zum Download zur Verfügung.

Sie können diese Datei gemäß der Hardware einer bestimmten Umgebung anpassen.

Hinweis: Wenn Sie eine angepasste Datei definieren, wird nur diese verwendet, nicht die in der .msi-Datei integrierte Datei. Die Standarddatei wird nur dann verwendet, wenn keine POA-Konfigurationsdatei definiert ist oder gefunden wird.

Um die POA-Konfigurationsdatei zu installieren, geben Sie folgenden Befehl ein:

MSIEXEC /i <Client-MSI-Paket> POACFG=<Pfad der POA-Konfigurationsdatei>

Weitere Informationen finden Sie in unserer Wissensdatenbank: http://www.sophos.com/support/knowledgebase/article/65700.html.

Die folgenden Hotkeys werden in der POA unterstützt:

- **Shift F3** = USB Legacy Unterstützung (An/Aus)
- **Shift F4**= VESA Grafikmodus (Aus/An)
- **Shift F5**= USB 1.x und 2.0 Unterstützung (Aus/An)
- **Shift F6** = ATA Controller (Aus/An))
- **Shift F7** = nur USB 2.0 Unterstützung (Aus/An)

  USB 1.x Unterstützung bleibt wie über Shift F5 gesetzt.
- **Shift F9** = ACPI/APIC (Aus/An)

USB Hotkeys Abhängigkeitsmatrix

Shift F3	Shift F5	Shift F7	Legacy	USB 1.x	USB 2.0	Comment
aus	aus	aus	an	an	an	3.
an	aus	aus	aus	an	an	Standard
aus	an	aus	an	aus	aus	1., 2.
an	an	aus	an	aus	aus	1., 2.
aus	aus	an	an	an	aus	3.
an	aus	an	aus	an	aus	
aus	an	an	an	aus	aus	
an	an	an	an	aus	aus	2.

1. Shift F5 deaktiviert sowohl die Unterstützung von USB 1.x als auch von USB 2.0.

Hinweis: Durch Drücken von Shift F5 reduziert sich die Wartezeit bis zum Starten der POA erheblich. Beachten Sie jedoch, dass bei Benutzung einer USB-Tastatur oder einer USB-Maus am betreffenden Benutzer-PC diese Geräte durch Drücken von Shift F5 möglicherweise deaktiviert werden.

2. Wenn die USB-Unterstützung nicht aktiviert ist, versucht die POA, BIOS SMM zu benutzen anstatt den USB-Controller zu sichern und wiederherzustellen. Der Legacy-Modus kann in diesem Szenario funktionieren.

3. Die Legacy-Unterstützung ist aktiviert, die USB-Unterstützung ist aktiviert. Die POA versucht, den USB-Controller zu sichern und wiederherzustellen. Der Computer kann sich je nach eingesetzer BIOS-Version aufhängen.

Es besteht die Möglichkeit, Änderungen, die über Hotkeys vorgenommen werden können, bei der Installation der SafeGuard Enterprise Verschlüsselungs-Software über eine mst Datei bereits vorzudefinieren. Verwenden Sie dazu den entsprechenden Aufruf in Verbindung mit msiexec.

NOVESA	Definiert, ob VESA oder VGA Modus verwendet werden. 0 = VESA Modus (Standard), 1 = VGA Modus
NOLEGACY	Definiert, ob nach der POA-Anmeldung Legacy-Unterstützung aktiviert ist. 0 = Legacy Support aktiviert, 1 = kein Legacy Support (Standard)
ALTERNATE:	Definiert, ob USB Geräte von der POA unterstützt werden. 0 = USB-Unterstützung ist aktiviert (Standard), 1 = keine USB-Unterstützung
NOATA	Definiert, ob der Int13 Gerätetreiber verwendet wird. 0 = Standard ATA Gerätetreiber (Standard), 1 = Int13 Gerätetreiber
ACPIAPIC	Definiert, ob die ACPI/APIC-Unterstützung benutzt wird. 0 = Keine ACPI/APIC-Unterstützung, 1 = ACPI/APIC-Unterstützung ist aktiv.
NOVESA	Definiert, ob VESA oder VGA-Modus verwendet wird. 0 = VESA-Modus (Standard), 1 = VGA-Modus

20.5 Deaktivierte POA und Lenovo Rescue and Recovery

Sollte auf dem Endpoint-Computer die Power-on Authentication deaktiviert sein, so sollte zum Schutz vor dem Zugriff auf verschlüsselte Dateien aus der Rescue and Recovery Umgebung heraus die Rescue and Recovery Authentisierung eingeschaltet sein.

Detaillierte Informationen zur Aktivierung der Rescue and Recovery Authentisierung finden Sie in der Lenovo Rescue and Recovery Dokumentation.

21 Recovery-Optionen

SafeGuard Enterprise bietet verschiedene Recovery-Optionen, die auf unterschiedliche Szenarien zugeschnitten sind:

- **Recovery für die Anmeldung über Local Self Help**

  Mit Local Self Help können sich Benutzer, die ihr Kennwort vergessen haben, ohne Unterstützung eines Helpdesks wieder an Ihrem Computer anmelden. So erhalten Benutzer auch in Situationen, in denen sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu ihrem Computer. Um sich anzumelden, müssen sie lediglich eine bestimmte Anzahl an vordefinierten Fragen in der Power-on Authentication beantworten.

  Local Self Help reduziert die Anzahl an Helpdesk-Anforderungen für Recovery-Vorgänge, die die Anmeldung betreffen. Helpdesk-Mitarbeitern werden somit Routine-Aufgaben abgenommen und sie können sich auf komplexere Support-Anforderungen konzentrieren.

  Für detaillierte Informationen, siehe *Recovery über Local Self Help* auf Seite 240.

- **Recovery über Challenge/Response**

  Das Challenge/Response-Verfahren ist ein sicheres und effizientes Recovery-System, das Benutzer unterstützt, die sich nicht mehr an ihrem Computer anmelden oder nicht mehr auf verschlüsselte Daten zugreifen können. Während eines Challenge/Response-Verfahrens übermittelt der Benutzer einen auf dem Endpoint-Computer erzeugten Challenge-Code an den Helpdesk-Beauftragten. Dieser erzeugt auf der Grundlage des Challenge-Codes einen Response-Code, der den Benutzer zum Ausführen einer bestimmten Aktion auf dem Computer berechtigt.

  Mit Recovery über Challenge/Response bietet SafeGuard Enterprise verschiedene Workflows für typische Recovery-Szenarien, für die die Unterstützung durch ein Helpdesk erforderlich ist.

  Für detaillierte Informationen, siehe *Recovery über Challenge/Response* auf Seite 246.

- **System-Recovery**

  SafeGuard Enterprise bietet verschiedene Methoden und Tools für Recovery-Vorgänge in Bezug auf wichtige System- und SafeGuard Enterprise Komponenten, z. B.:

  - Korrupter MBR
  - Probleme in Bezug auf den SafeGuard Enterprise Kernel
  - Probleme in Bezug auf Volume-Zugriff

- Probleme in Bezug auf Windows-Boot-Vorgänge
- Probleme in Bezug auf die GINA

Für detaillierte Informationen, siehe *Systemwiederherstellung* auf Seite 272.

22 Recovery über Local Self Help

SafeGuard Enterprise bietet für Endpoint-Computer die Funktion Local Self Help. Über Local Self Help können sich Benutzer, die Ihr Kennwort vergessen haben, ohne Unterstützung des Helpdesks wieder an ihrem Computer anmelden.

Mit Local Self Help erhalten Benutzer auch in Situationen, in denen sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu ihrem Computer. Um sich anzumelden, muss der Benutzer lediglich eine bestimmte Anzahl an vordefinierten Fragen in der Power-on Authentication beantworten.

Die zu beantwortenden Fragen können Sie als zuständiger Sicherheitsbeauftragter zentral vordefinieren und per Richtlinie an die Endpoint-Computer verteilen. Als Vorlage liefern wir Ihnen ein vordefiniertes Fragenthema, das Sie unverändert benutzen oder modifizieren können. Sie können die Benutzer auch per Richtlinie berechtigen, selbst Fragen zu definieren.

Für die initiale Beantwortung und spätere Bearbeitung der Fragen steht dem Benutzer nach der Aktivierung der Funktion auf seinem Computer der Local Self Help Assistent zur Verfügung. Detaillierte Informationen zu Local Self Help auf dem Endpoint-Computer finden Sie in der SafeGuard Enterprise Benutzer-Hilfe im Kapitel *Recovery über Local Self Help*.

Local Self Help reduziert die Anzahl an Helpdesk-Anforderungen für Notfälle, die die Anmeldung betreffen. Helpdesk-Mitarbeitern werden somit Routine-Aufgaben abgenommen und sie können sich auf komplexere Support-Anforderungen konzentrieren.

22.1 Parameter für Local Self Help über eine Richtlinie definieren

Die Einstellungen für Local Self Help definieren Sie in einer Richtlinie vom Typ **Allgemeine Einstellungen** unter **Recovery für die Anmeldung** - **Local Self Help aktivieren**. Hier aktivieren Sie die Funktion zur Benutzung auf den Endpoint-Computern und legen weitere Berechtigungen und Parameter fest.

22.1.1 Local Self Help aktivieren

Um die Funktion Local Self Help für die Benutzung auf Endpoint-Computern zu aktivieren, wählen Sie im Feld **Local Self Help** die Option **Local Self Help aktivieren**.

Nach dem Wirksamwerden der Richtlinie auf den Computern sind die Benutzer aufgrund dieser Einstellung berechtigt, Local Self Help für Recovery-Vorgänge, die die Anmeldung betreffen, zu benutzen. Hierzu müssen die Benutzer die Funktion auf Ihrem Computer durch Beantwortung der erhaltenen Fragen oder durch Erstellung und Beantwortung eigener Fragen (je nach Berechtigung) aktivieren.

Nach dem Erhalt der von Ihnen erstellten Richtlinie und dem Neustart des Computers steht den Benutzern dafür der Local Self Help Assistent über das System Tray Icon in der Windows Task-Leiste zur Verfügung.

22.1.2 Weitere Einstellungen definieren

Neben der Aktivierung von Local Self Help können Sie in einer Richtlinie vom Typ **Allgemeine Einstellung** folgende weiteren Einstellungen definieren:

- **Minimale Länge der Antwort**

  Legen Sie hier die Mindestlänge der Antworten in Zeichen fest. Die Standardeinstellung ist **1**.

- **Willkommenstext unter Windows**

  Hier können Sie einen individuellen Informationstext angeben, der beim Starten des Local Self Help Assistenten auf dem Benutzercomputer im ersten Dialog angezeigt werden soll. Dieser Text muss zuvor erstellt und registriert werden.

- **Benutzer dürfen eigene Fragen festlegen**

  Für die Hinterlegung der Fragen und Antworten für Local Self Help gibt es folgende Möglichkeiten:

  - Sie definieren als Sicherheitsbeauftragter die Fragen und verteilen Sie an die Benutzer. Die Benutzer sind nicht dazu berechtigt, eigene Fragen zu definieren.
  - Sie definieren als Sicherheitsbeauftragter die Fragen und verteilen Sie an die Benutzer. Die Benutzer sind dazu berechtigt, zusätzlich eigene Fragen zu definieren. Bei der Beantwortung der für die Aktivierung von Local Self Help notwendigen Mindestanzahl an Fragen können die Benutzer zwischen vorgegebenen und eigenen Fragen wählen oder eine Kombination aus beiden verwenden.

- Sie berechtigen die Benutzer dazu, eigene Fragen zu definieren und geben keine vordefinierten Fragen vor. Die Benutzer aktivieren Local Self Help durch Definition und Beantwortung eigener Fragen.

Um die Benutzer zur Definition eigener Fragen zu berechtigen, wählen Sie im Feld **Benutzer dürfen eigene Fragen festlegen** die Einstellung **Ja**.

22.2 Fragen definieren

Voraussetzung dafür, dass Local Self Help auf dem Endpoint-Computer verwendet werden kann, ist die Hinterlegung von mindestens zehn beantworteten Fragen. Um sich über Local Self Help an der Power-on Authentication anzumelden, muss der Benutzer fünf Fragen, die per Zufallsprinzip aus diesen zehn Fragen ausgewählt werden, korrekt beantworten.

Wenn der Benutzer nicht dazu berechtigt ist, eigene Fragen zu definieren, müssen Sie mindestens zehn vordefinierte Fragen mit der Richtlinie an den Endpoint-Computer für die Aktivierung von Local Self Help weitergeben.

Für die Definition und Bearbeitung von Local Self Help Fragen benötigen Sie als Sicherheitsbeauftragter die Berechtigung **Local Self Help Fragen modifizieren**.

22.2.1 Vorlage verwenden

Für Local Self Help liefern wir Ihnen ein vordefiniertes Fragenthema. Dieses Fragenthema steht standardmäßig in den Sprachen Deutsch und Englisch im Richtlinien-Navigationsbereich unter **Local Self Help Fragen** zur Verfügung.

Das Fragenthema steht optional auch in den Sprachen Französisch, Italienisch, Spanisch und Japanisch zur Verfügung. Diese Sprachversionen lassen sich zusätzlich in den Navigationsbereich importieren.

Hinweis: Bei der Eingabe von Antworten auf Japanisch zur Aktivierung von Local Self Help auf Endpoint-Computern müssen die Benutzer Romajii-Zeichen (römische/lateinische Zeichen) verwenden. Andernfalls wird bei der Eingabe der Antworten in der Power-on Authentication keine Übereinstimmung erreicht.

Sie können das vordefinierte Fragenthema unverändert verwenden, bearbeiten oder löschen.

Wenn Sie die beiden Sprachversionen des vordefinierten Fragenthemas unverändert belassen und Local Self Help über eine Richtlinie vom Typ **Allgemeine Einstellungen**, werden die beiden vordefinierten Fragenthemen automatisch mit dieser Richtlinie an die Endpoint-Computer weitergegeben.

22.3 Fragenthemen importieren

Über den Importvorgang können Sie zusätzliche Sprachversionen des vordefinierten Fragenthemas (oder eigene, als .XML-Datei erstellte Fragenlisten) importieren.

So importieren Sie ein Fragenthema:

1. Erstellen Sie ein neues Fragenthema (siehe *Neues Fragenthema erstellen und Fragen hinzufügen*, Seite 243).
2. Markieren Sie im **Richtlinien** Navigationsbereich das neue Fragenthema unter **Local Self Help Fragen**.
3. Klicken Sie im Arbeitsbereich mit der rechten Maustauste. Das Kontextmenü für das Fragenthema wird geöffnet. Wählen Sie **Importieren**.
4. Wählen Sie das Verzeichnis, in dem das Fragenthema abgelegt ist, sowie das gewünschte Fragenthema und klicken Sie auf **Öffnen**.

Die importierten Fragen werden im Arbeitsbereich angezeigt. Sie können das Fragenthema nun unverändert speichern oder bearbeiten.

22.4 Neues Fragenthema erstellen und Fragen hinzufügen

Neben Fragenthemen in verschiedenen Sprachen können Sie auch neue Fragenthemen zu unterschiedlichen Themenbereichen erstellen. Somit können Sie Benutzern mehrere Fragenthemen zur Verfügung stellen, aus denen das für sie am besten geeignete Thema auswählen können.

So erstellen Sie ein neues Fragenthema und fügen Fragen hinzu:

1. Markieren Sie im **Richtlinien** Navigationsbereich den Eintrag **Local Self Help Fragen**.
2. Klicken Sie mit der rechten Maustaste auf **Local Self Help Fragen** und wählen Sie **Neu** > **Fragenthema**.
3. Geben Sie einen Namen für das Fragenthema ein und klicken Sie auf **OK**.
4. Markieren Sie im **Richtlinien** Navigationsbereich das neue Fragenthema unter **Local Self Help Fragen**.
5. Klicken Sie im Arbeitsbereich mit der rechten Maustaste. Das Kontextmenü für das Fragenthema wird geöffnet. Wählen Sie **Hinzufügen**.

6. Eine neue Fragenzeile wird hinzugefügt. Geben Sie Ihre Frage ein und drücken Sie **Enter**. Um weitere Fragen hinzufügen, wiederholen Sie diesen Vorgang.
7. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern**-Symbol in der Symbolleiste klicken.

Ihr Fragenthema ist registriert und wird der Richtlinie vom Typ **Allgemeine Einstellungen**, über die Local Self Help auf den Endpoint-Computern aktiviert wird, automatisch mitgegeben.

22.5 Fragenthemen bearbeiten

So bearbeiten Sie bereits vorhandene Fragenthemen:

1. Markieren Sie das gewünschte Fragenthema unter **Local Self Help Fragen** im **Richtlinien** Navigationsbereich.
2. Sie können nun Fragen hinzufügen, ändern oder löschen.
   - Um Fragen hinzuzufügen, klicken Sie im Arbeitsbereich mit der rechten Maustaste und wählen Sie im Kontextmenü **Hinzufügen**. Geben Sie nun in der neu angezeigten Zeile Ihre Frage ein.
   - Um Fragen zu ändern, klicken Sie auf den Fragentext im Arbeitsbereich. Bei der gewählten Frage wird ein Stiftsymbol angezeigt. Geben Sie auf der Fragenzeile Ihre Änderungen ein.
   - Um Fragen zu löschen, markieren Sie die gewünschte Frage durch Klicken auf das graue Kästchen zu Beginn der Fragenzeile im Arbeitsbereich und wählen Sie im Kontextmenü des Frageneintrags **Löschen**.
3. Speichern Sie Ihre Änderungen an der Fragenliste, indem Sie auf das **Speichern**-Symbol in der Symbolleiste klicken.

Das geänderte Fragenthema ist registriert und wird der Richtlinie vom Typ **Allgemeine Einstellungen**, über die Local Self Help auf den Endpoint-Computern aktiviert wird, automatisch mitgegeben.

22.6 Fragenthemen löschen

Um ein Fragenthema zu löschen, klicken Sie mit der rechten Maustaste auf das Fragenthema unter **Local Self Help Fragen** im **Richtlinien** Navigationsbereich und wählen Sie **Löschen**.

Hinweis: Wenn Sie ein Fragenthema löschen, nachdem die Benutzer bereits Fragen aus diesem Thema zur Aktivierung von Local Self Help auf ihren Computern beantwortet haben, werden die Antworten der Benutzer ungültig, da die Fragen nicht mehr vorhanden sind.

22.7 Willkommenstexte registrieren

Sie können im Richtlinien-Navigationsbereich des SafeGuard Management Center einen Willkommenstext registrieren, der im ersten Dialog des Local Self Help Assistenten angezeigt werden soll.

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Informationstexte beträgt 50 KB. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden Sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Konvertierung durchgeführt wird, werden Sie durch eine Meldung darüber informiert.

So registrieren Sie Informationstexte:

1. Klicken Sie im **Richtlinien** Navigationsbereich mit der rechten Maustaste auf **Informationstext** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzeigenden Text ein.
3. Wählen Sie über die Schaltfläche **[...]** die zuvor erstellte Textdatei aus. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Informationstext** im **Richtlinien** Navigationsbereich. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

23 Recovery über Challenge/Response

Zur Optimierung von Workflows im Unternehmen und zur Reduzierung von Helpdesk-Kosten bietet SafeGuard Enterprise eine Challenge/Response Recovery-Lösung. Mit einem benutzerfreundlichen Challenge/Response-Verfahren unterstützt SafeGuard Enterprise Benutzer, die sich an ihrem Computer nicht mehr anmelden oder nicht auf verschlüsselte Daten zugreifen können.

Diese Funktionalität ist im SafeGuard Management Center in Form eines Recovery-Assistenten integriert.

23.1 Nutzen und Vorteile des Challenge/Response-Verfahrens

Das Challenge/Response-Verfahren ist ein sicheres und effizientes Notfallsystem.

- Während des gesamten Vorgangs werden keine vertraulichen Daten in unverschlüsselter Form ausgetauscht.
- Informationen, die unberechtigte Dritte durch Mitverfolgen dieses Vorgangs erhalten könnten, lassen sich weder zu einem späteren Zeitpunkt noch auf anderen Geräten verwenden.
- Für den Computer, auf den zugegriffen wird, ist keine Online-Netzwerkverbindung erforderlich. Der Response Code Assistent für den Helpdesk läuft auch auf einem Standalone-Computer ohne Verbindung zum SafeGuard Enterprise Server. Eine komplexe Infrastruktur ist nicht erforderlich.
- Der Benutzer kann schnell wieder mit dem Computer arbeiten. Es gehen keine verschlüsselten Daten verloren, nur weil der Benutzer das Kennwort vergessen hat.

23.2 Typische Situationen, in denen Hilfe beim Helpdesk angefordert wird

- Ein Benutzer hat sein Kennwort für die Anmeldung vergessen. Der Computer ist gesperrt.
- Der Local Cache der Power-on Authentication ist teilweise beschädigt.
- Ein Benutzer ist krank oder im Urlaub und ein Kollege muss auf die Daten auf dem Computer zugreifen.
- Ein Benutzer möchte auf ein Volume zugreifen, das mit einem Schlüssel verschlüsselt ist, der auf dem Computer nicht verfügbar ist.

SafeGuard Enterprise bietet für diese typischen Szenarien unterschiedliche Recovery-Workflows, die dem Benutzer wieder den Zugang zu seinem Computer ermöglichen.

23.3 Challenge/Response Workflow

Das Challenge/Response-Verfahren basiert auf zwei Komponenten:

- Endpoint-Computer, auf dem der Challenge Code erzeugt wird.
- SafeGuard Management Center, in dem Sie als Helpdesk-Beauftragter mit ausreichenden Rechten einen Response-Code erstellen, der den Benutzer zur Ausführung der angeforderten Aktion auf dem Computer berechtigt.

1. Der Benutzer fordert auf seinem Computer einen Challenge-Code an. Je nach Recovery-Typ wird der Challenge-Code in der Power-on Authentication oder über das KeyRecovery Tool angefordert.

Ein Challenge-Code in Form einer ASCII-Zeichenfolge wird generiert und angezeigt.

2. Der Benutzer wendet sich an den Helpdesk und übermittelt seine notwendige Identifikation sowie den Challenge-Code.
3. Der Helpdesk-Beauftragte startet den Recovery-Assistenten im SafeGuard Management Center.
4. Der Helpdesk-Beauftragte wählt den entsprechenden Recovery-Typ, bestätigt die Identifikationsinformationen sowie den Challenge-Code und wählt die gewünschte Recovery-Aktion aus.

Ein Response-Code in Form einer ASCII-Zeichenfolge wird generiert und angezeigt.

5. Der Helpdesk-Beauftragte übermittelt dem Benutzer den Response-Code, z. B. über das Telefon oder über eine Textmitteilung.
6. Der Benutzer gibt den Response-Code ein. Je nach Recovery-Typ erfolgt dies in der POA oder über das KeyRecovery Tool.

Der Benutzer kann die autorisierte Aktion, z. B. Rücksetzen des Kennworts, ausführen und wieder mit dem Computer arbeiten.

23.4 Wann muss der Benutzer sein Kennwort ändern?

Im Rahmen eines SafeGuard Enterprise Recovery-Vorgangs muss der Benutzer u. U. sein Windows-Kennwort ändern. Die folgende Tabelle zeigt, wann es erforderlich ist, das Kennwort zu ändern. Die ersten vier Spalten zeigen spezifische Bedingungen, die während des Challenge/Response-Verfahrens auftreten können. Die letzte Spalte gibt basierend auf den Bedingungen aus den ersten vier Spalten an, ob der Benutzer sein Kennwort ändern muss.

Bedingung: C/R mit Benutzeranmeldung und Anzeige des Kennworts	Bedingung: C/R mit Benutzeranmeldung	Bedingung: Domänen-Controller verfügbar	Bedingung: Option zur Kennwortanzeige vom Benutzer abgelehnt	Ergebnis: Benutzer muss sein Windows-Kennwort ändern
Ja	Ja	Ja	Nein	**Nein**
Ja	Ja	Ja	Ja	**Ja**
Ja	Ja	Ja	Ja	**Nein**
Nein	Ja	Ja	entf.	**Ja**
Nein	Ja	Nein	entf.	**Nein**
Nein	Nein	Nein	entf.	**Nein**

23.5 Recovery-Assistenten starten

Damit Sie in der Lage sind, ein Recovery-Verfahren auszuführen, stellen Sie sicher, dass sie über die erforderlichen Rechte und Berechtigungen verfügen.

1. Melden Sie sich am SafeGuard Management Center an.
2. Klicken Sie auf **Extras** > **Recovery** in der Menüleiste.

Der SafeGuard Recovery-Assistent wird gestartet. Sie können den angeforderten Recovery-Typ auswählen.

23.6 Recovery-Typen

Wählen Sie den Recovery-Typ, den Sie verwenden möchten. Folgende Recovery-Typen stehen zur Verfügung:

- **Challenge/Response für SafeGuard Enterprise Clients (Managed)**

  Challenge/Response für zentral durch das SafeGuard Management Center verwaltete Computer. Die Computer sind im Bereich **Benutzer & Computer** im SafeGuard Management Center aufgelistet.

- **Challenge/Response mit virtuellen Clients**

  Recovery-Vorgänge für verschlüsselte Volumes lassen sich in Fällen, in denen ein Challenge/Response-Vorgang normalerweise nicht unterstützt würde (z. B. bei einer korrupten POA), auf einfache Art und Weise unter Anwendung von spezifischen Dateien mit der Bezeichnung virtuelle Clients durchführen.

- **Challenge/Response for Sophos SafeGuard Clients (Standalone)**

  Challenge/Response für lokal verwaltete Computer. Diese Computer haben nie eine Verbindung zum SafeGuard Enterprise Server. Für jeden dieser Computer wird während der Konfiguration eine Schlüssel-Recovery-Datei generiert. Diese Datei enthält den definierten Computerschlüssel, der mit dem Unternehmenszertifikat verschlüsselt ist. Wenn diese Datei für den Zugriff durch den Helpdesk-Beauftragten zur Verfügung steht, z. B. auf einem USB-Stick oder über eine Netzwerkfreigabe, wird das Challenge/Response-Verfahren für einen Standalone-Computer unterstützt.

Hinweis: Darüber hinaus steht das Recovery-Verfahren Local Self Help zur Verfügung, für das keine Unterstützung durch den Helpdesk benötigt wird.

23.7 Recovery über Challenge/Response für SafeGuard Enterprise Clients

SafeGuard Enterprise bietet ein Recovery-Verfahren für in der Datenbank registrierte Endpoint-Computer für verschiedene Notfallszenarien, z. B. Kennwort-Recovery oder Zugriff auf Daten durch Booten von einem externen Medium.

Das Challenge/Response-Verfahren wird sowohl für native SafeGuard Enterprise Computer als auch für mit BitLocker verschlüsselte Endpoint-Computer unterstützt. Während des Challenge/Response-Verfahrens wird automatisch erkannt, welcher Computertyp in Gebrauch ist. Der Recovery-Workflow wird entsprechend angepasst.

23.7.1 Recovery-Aktionen für SafeGuard Enterprise Clients

Der Recovery Workflow richtet sich danach, für welchen Typ von Endpoint-Computer das Recovery-Verfahren angefordert wird.

Hinweis: Für mit BitLocker verschlüsselte Computer steht als Recovery-Aktion nur die Wiederherstellung des Schlüssels, der für die Verschlüsselung eines spezifischen Volumes verwendet wurde, zur Verfügung. Eine Recovery-Aktion für Kennwörter ist nicht verfügbar.

23.7.1.1 Kennwort auf POA-Ebene wiederherstellen

Einer der am häufigsten auftretenden Recovery-Szenarien besteht darin, dass Benutzer ihr Kennwort vergessen haben. SafeGuard Enterprise wird standardmäßig mit aktivierter Power-on Authentication (POA) installiert. Das POA-Kennwort, mit dem auf den Computer zugegriffen wird, ist identisch mit dem Windows-Kennwort.

Wenn der Benutzer das Kennwort auf der POA-Ebene vergessen hat, generiert der Helpdesk-Beauftragte eine Response mit der Option **SGN Client mit Benutzeranmeldung booten**, ohne das Benutzerkennwort anzuzeigen.

In diesem Fall startet der Computer jedoch nach Eingabe des Response-Codes bis zur Betriebssystemebene. Der Benutzer muss somit unter der Voraussetzung, dass Zugriff auf die Domäne besteht, das Kennwort auf Windows-Ebene ändern. Danach kann der Benutzer sich sowohl an Windows als auch an der Power-on Authentication mit dem neuen Kennwort anmelden.

Best practice zur Wiederherstellung des Kennworts auf POA-Ebene

Hinweis: Wir empfehlen, in erster Linie die folgenden Methoden einzusetzen, um ein vergessenes Kennwort wiederherzustellen, damit das Kennwort nicht zentral zurückgesetzt werden muss:

Verwenden Sie Local Self Help. Mit Recovery über Local Self Help kann der Benutzer selbst ohne die Unterstützung des Helpdesk das vergessene Kennwort anzeigen lassen und es weiterverwenden, ohne es zurücksetzen zu müssen. Für weitere Informationen siehe *Recovery über Local Self Help* auf Seite 4.

Beim Einsatz von Challenge/Response: Wir raten davon ab, das Kennwort zentral im Active Directory zurückzusetzen, bevor das Challenge/Response-Verfahren gestartet wird. Damit bleibt gewährleistet, dass das Kennwort zwischen Windows und Sophos SafeGuard weiterhin synchronisiert ist. Stellen Sie sicher, dass der Helpdesk entsprechend informiert ist.

Generieren Sie als SafeGuard Enterprise Helpdesk-Beauftragter eine Response mit der Option **SGN Client mit Benutzeranmeldung booten** und **Benutzerkennwort anzeigen**. Dies bietet den Vorteil, dass das Kennwort nicht im Active Directory geändert werden muss. Benutzer können mit dem alten Kennwort weiterarbeiten und es gegebenenfalls später lokal ändern.

23.7.1.2 Benutzerkennwort anzeigen

SafeGuard Enterprise bietet Benutzern die Möglichkeit, sich ihr Kennwort während des Challenge/Response-Verfahrens anzeigen zu lassen. Dies bietet den Vorteil, dass das Kennwort nicht im Active Directory geändert werden muss. Diese Option ist verfügbar, wenn die Anforderung **SGN Client mit Benutzeranmeldung booten** gestellt wird.

23.7.1.3 Ein anderer Benutzer muss den durch SafeGuard Enterprise geschützten Computer booten

In diesem Fall bootet der Benutzer, der Zugriff auf den Computer benötigt, den Computer und gibt seinen Benutzernamen ein. Der Benutzer fordert dann eine Challenge an. Der SafeGuard Helpdesk generiert eine Response vom Typ **SGN Client mit Benutzeranmeldung booten** mit **aktivierter durchgehender Anmeldung an Windows**. Der Benutzer wird angemeldet und kann den Computer benutzen.

23.7.1.4 Zugriff auf Daten durch Booten von externem Medium oder Diskette

Mit Hilfe des Challenge/Response-Verfahrens lässt sich ein Computer auch von einem externen Medium wie WinPE booten. Hierzu muss der Benutzer im POA-Anmeldedialog die Option **Weiterbooten von: Diskette/externem Medium** wählen und eine Challenge starten. Nach Erhalt der Response kann der Benutzer die Anmeldeinformationen wie gewohnt in der POA eingeben und den Boot-Vorgang von einem externen Medium fortsetzen.

Für den Zugriff auf ein verschlüsseltes Volume müssen folgende Voraussetzungen erfüllt sein:

- Das zu verwendende Gerät muss den SafeGuard Enterprise Filtertreiber enthalten. Eine detaillierte Beschreibung zum Erstellen einer solchen Treiber-CD finden Sie in unserer Wissensdatenbank:

  http://www.sophos.com/support/knowledgebase/article/108805.html

- Der Benutzer muss von einem externen Medium booten und muss die hierzu erforderliche Berechtigung haben. Diese Berechtigung wird erteilt, indem man im SafeGuard Management Center eine Richtlinie erstellt und diese dem Client zuweist. (Richtlinie Authentisierung > Zugriff: Benutzer kann nur von Festplatte booten auf „Nein“ setzen). Standardmäßig ist die Berechtigung zum Booten von externen Medien nicht zugewiesen.

- Der Endpoint-Computer muss den Boot-Vorgang von einem anderen Medium als einer Festplatte generell unterstützen.

- Es kann nur auf Volumes, die mit dem definierten Computerschlüssel verschlüsselt sind, zugegriffen werden. Dieser Verschlüsselungstyp kann in einer Geräteschutzrichtlinie im SafeGuard Management Center definiert und dem Client zugewiesen werden.

Bitte beachten Sie, dass bei Anwendung von externen Medien wie WinPE für den Zugriff auf ein verschlüsseltes Laufwerk der Zugriff auf das Volume nur teilweise gewährt wird.

23.7.1.5 SafeGuard Enterprise Local Cache wiederherstellen

Dieser Vorgang ist notwendig, wenn der SafeGuard Enterprise Local Cache beschädigt ist. Im Local Cache werden alle Schlüssel, Richtlinien, Benutzertifikate und Audit-Dateien gespeichert. Standardmäßig ist in diesem Fall der Recovery-Vorgang deaktiviert, d. h. der Local Cache wird automatisch aus seiner Sicherungskopie wiederhergestellt. In diesem Fall ist kein Challenge/Response-Verfahren für die Reparatur notwendig. Soll die Reparatur des Local Cache explizit über ein Challenge/Response-Verfahren durchgeführt werden, kann der Recovery-Vorgang über eine Richtlinie aktiviert werden. In diesem Fall wird der Benutzer automatisch bei der Anmeldung an der Power-on Authentication aufgefordert, ein Challenge/Response-Verfahren zu starten.

23.7.2 Response für SafeGuard Enterprise Clients

Um für einen SafeGuard Enterprise Client eine Response in einem Challenge/Response-Verfahren zu generieren, werden der Name des betreffenden Endpoint-Computers und die Domäne benötigt:

Hinweis: Der Name muss immer der Distinguished Name des Computers sein.

1. Wählen Sie **SafeGuard Enterprise Client** (**Managed**) im Dialog **Recovery-Typ**.

2. Wählen Sie die Domäne aus der Liste aus.

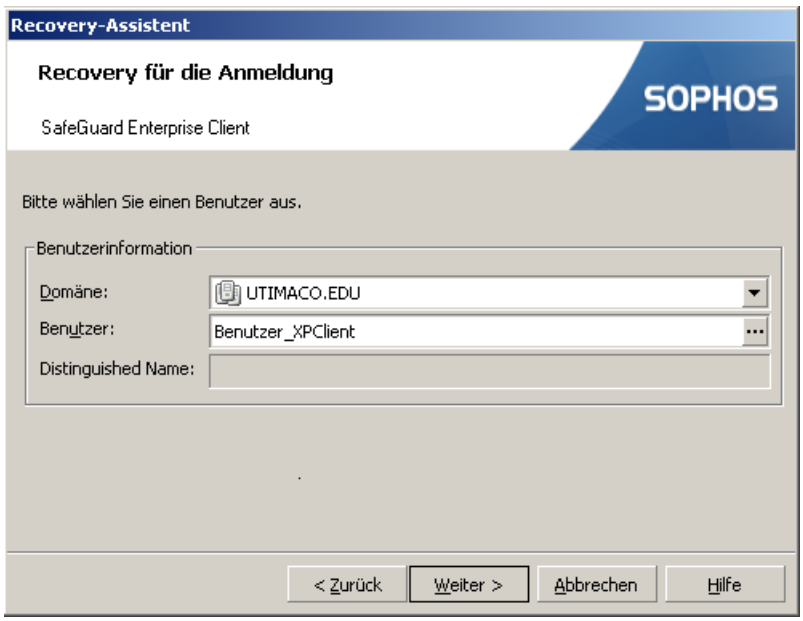
3. Wählen Sie den Computernamen. Hierzu gibt es mehrere Möglichkeiten:
   - Wählen Sie einen Namen, indem Sie auf **[...]** im Abschnitt **Computer-Information** des Dialogs **Recovery-Typ** klicken und anschließend **Jetzt suchen** klicken. Eine Liste mit Computern wird angezeigt. Wählen Sie den gewünschten Computer aus und klicken Sie auf **OK**. Der Computername wird nun im Fenster **Recovery-Typ** unter **Domäne** angezeigt.
   - Geben Sie den Kurznamen des Computers ein. Wenn Sie auf **Weiter** klicken, wird der Name in der Datenbank gesucht. Der gefundene Computername wird als Distinguished Name angezeigt.
   - Geben Sie den Computernamen direkt als Distinguished Name ein, zum Beispiel:

     ```
     CN=Desktop1,OU=Development,OU=Headquarter,DC=Sophos,DC=edu
     ```
4. Klicken Sie auf **Weiter**.

Das Programm bestimmt nun automatisch, ob es sich um einen nativen SafeGuard Enterprise Computer oder um einen mit BitLocker verschlüsselten Computer handelt, und passt den Recovery Workflow entsprechend an. Im Falle eines nativen SafeGuard Enterprise Computers wird im nächsten Schritt die Auswahl der Benutzerinformationen verlangt.

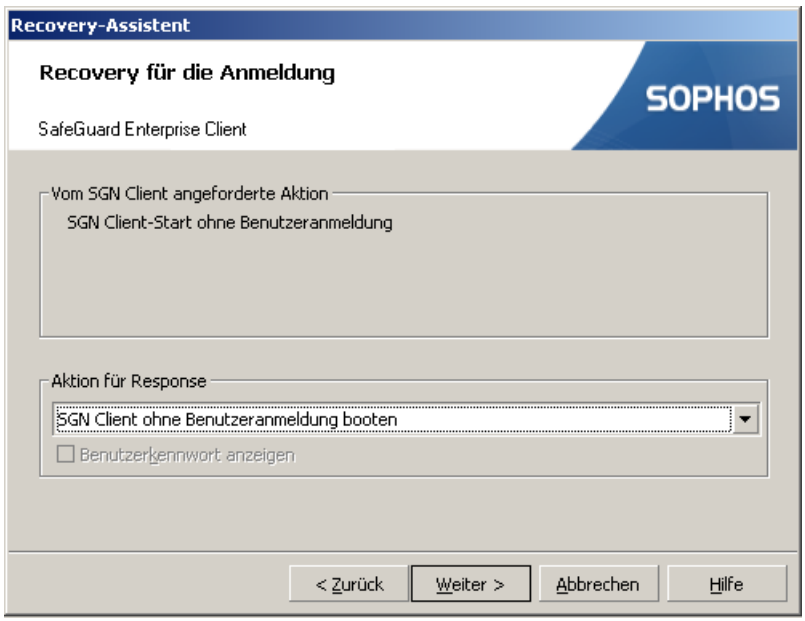
Nachdem der Computer in der Datenbank gefunden wurde, wird nun der entsprechende Benutzername und die Domäne für das Recovery eines SafeGuard Enterprise Clients benötigt.

1. Wählen Sie die Domäne des Benutzers.
2. Geben Sie den Benutzernamen ein. Hierfür gibt es mehrere Möglichkeiten:
   - Wählen Sie den Benutzernamen, indem Sie auf **[...]** im Abschnitt **Benutzerinformation** des Dialogs **Recovery für die Anmeldung** klicken und anschließend **Jetzt suchen** klicken. Eine Liste mit Benutzernamen wird angezeigt. Wählen Sie den gewünschten Namen und klicken Sie auf **OK**. Der Name wird unter **Domäne** im Recovery-Typ-Fenster angezeigt.
   - Geben Sie den Benutzernamen direkt ein. Stellen Sie sicher, dass der Name korrekt geschrieben ist.



3. Klicken Sie auf **Weiter**. Ein Fenster für die Eingabe des Challenge-Codes wird angezeigt.
4. Geben Sie den Challenge-Code ein, den der Benutzer Ihnen genannt hat, und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft. Wenn er falsch eingegeben wurde, wird der Hinweis `Ungültig` unterhalb des fehlerhaften Blocks angezeigt.

5. Wenn der Challenge-Code korrekt eingegeben wurde, werden die vom SafeGuard Enterprise Client angeforderte Aktion sowie die möglichen Recovery-Aktionen auf dem Client angezeigt. Die möglichen Response-Aktionen richten sich nach den Aktionen, die auf Client-Seite beim Aufrufen der Challenge angefordert wurden. Wenn auf Client-Seite zum Beispiel **Crypto Token erforderlich** angefordert wurde, stehen für die Response die Aktionen **SGN Client mit Benutzeranmeldung booten** und **SGN Client ohne Benutzeranmeldung booten** zur Verfügung.

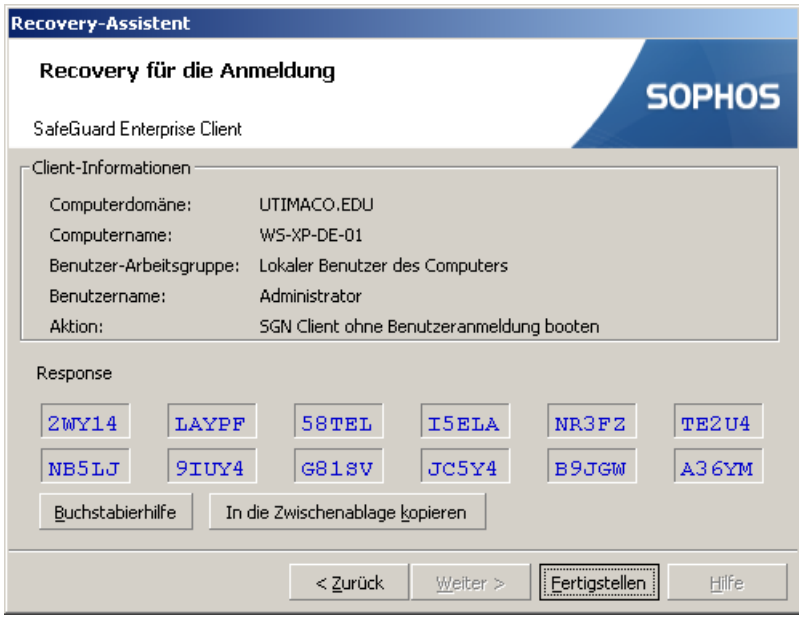


6. Wählen Sie die Aktion, die der Benutzer ausführen soll.

7. Wenn Sie **SGN Client mit Benutzeranmeldung booten** als Response-Aktion ausgewählt haben, können Sie zusätzlich auch die Option **Benutzerkennwort anzeigen** wählen, um das Kennwort auf dem Zielcomputer anzeigen zu lassen.

8. Klicken Sie auf **Weiter**.

9. Ein Response-Code wird generiert. Teilen Sie den Response-Code dem Benutzer mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.



Der Benutzer kann nun den Response-Code eingeben und die autorisierte Aktion durchführen.

23.8 Response für mit BitLocker verschlüsselte SafeGuard Enterprise Clients

Für mit BitLocker verschlüsselte Computer lässt sich ein Volume, auf das nicht mehr zugegriffen werden kann, wiederherstellen.

Hinweis: Der Name muss immer der Distinguished Name des Computers sein.

1. Wählen Sie im Fenster **Recovery-Typ** die Option **SafeGuard Enterprise Client**.
2. Wählen Sie die Domäne aus der Liste.
3. Geben Sie den Computernamen ein. Hierfür gibt es mehrere Möglichkeiten:
   - Wählen Sie einen Namen, indem Sie auf **[...]** im Abschnitt Computer-Information des Dialogs Recovery-Typ klicken und anschließend **Jetzt suchen** klicken. Eine Liste mit Computern wird angezeigt. Wählen Sie den gewünschten Computer aus und klicken Sie auf **OK**. Der Computername wird nun im Fenster **Recovery-Typ** unter **Domäne** angezeigt.
   - Geben Sie den Kurznamen des Computers ein. Wenn Sie auf **Weiter** klicken, wird der Name in der Datenbank gesucht. Der gefundene Computername wird als Distinguished Name angezeigt.
   - Geben Sie den Computernamen direkt als Distinguished Name ein, zum Beispiel:

     ```
     CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=edu
     ```

4. Klicken Sie auf **Weiter**.

Das Programm bestimmt nun automatisch, ob es sich um einen nativen SafeGuard Enterprise Computer oder um einen mit BitLocker verschlüsselten Computer handelt und passt den Recovery Workflow entsprechend an. Handelt es sich um einen mit BitLocker verschlüsselten Computer, so muss im nächsten Schritt das erforderliche Volume ausgewählt werden.

Nachdem der betreffende Computer in der Datenbank gefunden wurde, muss das Volume ausgewählt werden, für das die Recovery-Aktion am mit BitLocker verschlüsselten Endpoint-Computer durchgeführt werden soll.

1. Wählen Sie das Volume, auf das zugegriffen werden soll, aus der Liste und klicken Sie auf **Weiter**.
2. Der Recovery-Assistent zeigt nun den 48-stelligen Recovery-Schlüssel an.
3. Teilen Sie dem Benutzer diesen Schlüssel mit.

Der Benutzer kann nun den Schlüssel eingeben, um den Zugriff auf das mit BitLocker verschlüsselte Volume auf dem Endpoint-Computer wiederherzustellen.

23.9 Challenge/Response mit virtuellen Clients

Mit Recovery über Challenge/Response mit virtuellen Clients bietet SafeGuard Enterprise ein Recovery-Verfahren für verschlüsselte Volumes in komplexen Notfallsituationen, z. B., wenn die POA korrupt ist. Dieses Verfahren lässt sich sowohl auf zentral verwaltete Computer als auch auf Standalone-Computer anwenden.

Hinweis: Recovery mit virtuellen Clients sollte nur in komplexen Notfallsituationen angewendet werden. Wenn zum Beispiel nur ein Schlüssel für die Wiederherstellung eines Volumes fehlt, ist es am besten, den fehlenden Schlüssel dem Schlüsselbund des entsprechenden Benutzers zuzuweisen, um den Zugriff auf das Volume zu ermöglichen.

23.9.1 Recovery Workflow mit virtuellen Clients

Über folgenden allgemeinen Workflow lässt sich der Zugang zum verschlüsselten Computer wiederherstellen:

1. Sie erhalten die SafeGuard Enterprise Recovery Disk vom technischen Support.
2. Für den Helpdesk steht die Windows PE Recovery Disk mit den aktuellen SafeGuard Enteprise Filter-Treibern auf der Sophos Support-Website zum Download zur Verfügung. Weitere Informationen finden Sie in der Wissensdatenbank: http://www.sophos.com/support/knowledgebase/article/108805.html.
3. Erstellen Sie den virtuellen Client im SafeGuard Management Center.
4. Exportieren Sie den virtuellen Client in eine Datei.
5. Booten Sie den Computer von der Recovery Disk.
6. Importieren Sie die Datei mit dem virtuellen Client in das KeyRecovery Tool.
7. Starten Sie die Challenge im KeyRecovery Tool.
8. Bestätigen Sie den virtuellen Client im SafeGuard Management Center.
9. Wählen Sie die erforderliche Recovery-Aktion.
10. Geben Sie den Challenge-Code im SafeGuard Management Center ein.
11. Generieren Sie den Response-Code im SafeGuard Management Center.
12. Geben Sie den Response-Code im KeyRecovery Tool ein.

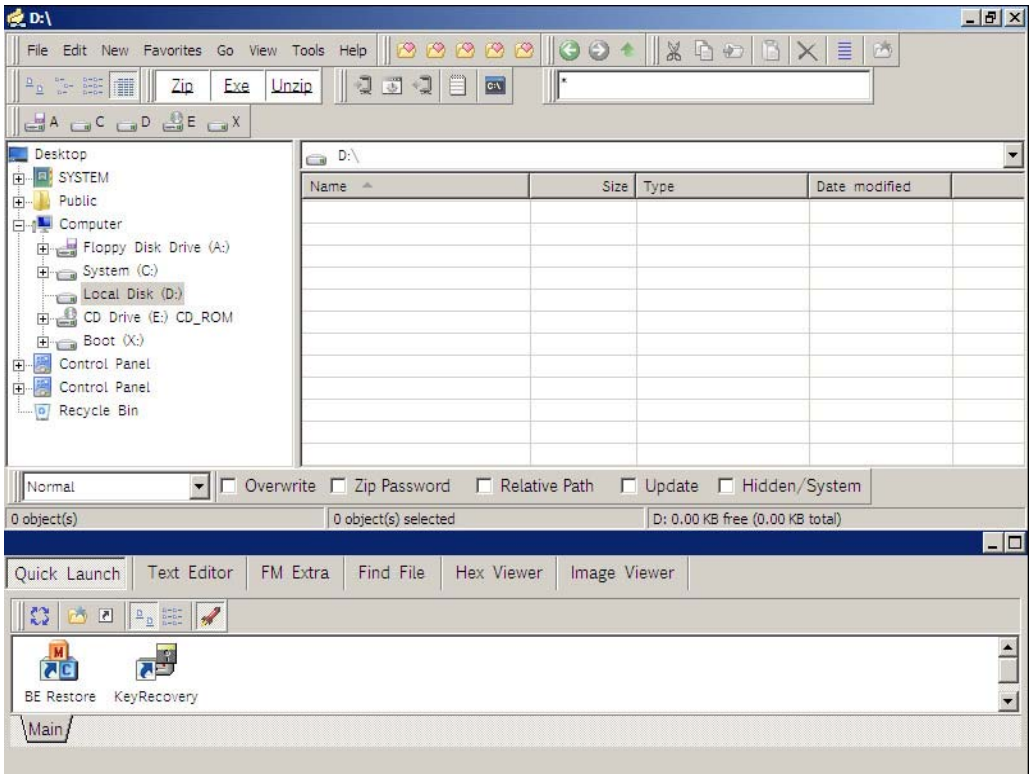
Auf den Computer kann wieder zugegriffen werden.

23.9.2 Computer von der Recovery Disk booten

Voraussetzung:

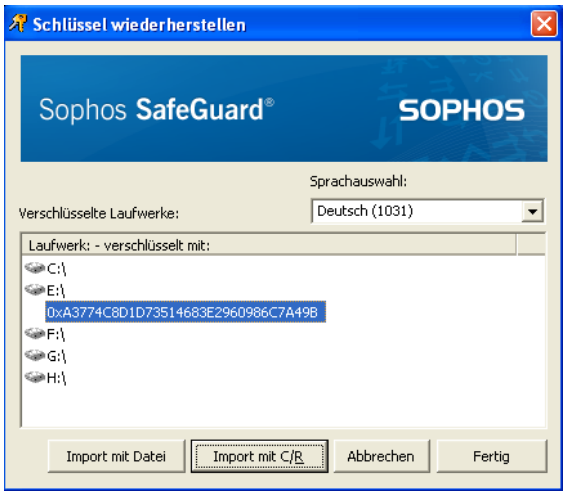
Stellen Sie sicher, dass die Boot-Reihenfolge im BIOS das Booten von CD erlaubt.

1. Legen Sie auf dem Endpoint-Computer die Recovery Disk ein und starten Sie den Computer. Der integrierte Dateimanager wird geöffnet. Hier sehen Sie auf einen Blick die bereitgestellten Volumes und Laufwerke.



Der Inhalt des verschlüsselten Laufwerks ist im Dateimanager nicht sichtbar. In den Eigenschaften des verschlüsselten Laufwerks werden weder das Dateisystem, noch die Kapazität sowie der verwendete/freie Speicherplatz angegeben.

2. Klicken Sie unten im Bereich **Quick Launch** des Dateimanagers auf das KeyRecovery-Symbol, um das KeyRecovery Tool zu öffnen. Das Key Recovery Tool zeigt dieSchlüssel-ID verschlüsselter Laufwerke.



3. Suchen Sie nach der Schlüssel-ID des Laufwerks, auf das Sie zugreifen möchten. Die Schlüssel-ID wird später abgefragt.

Im nächsten Schritt importieren Sie den virtuellen Client in das Key Recovery Tool.

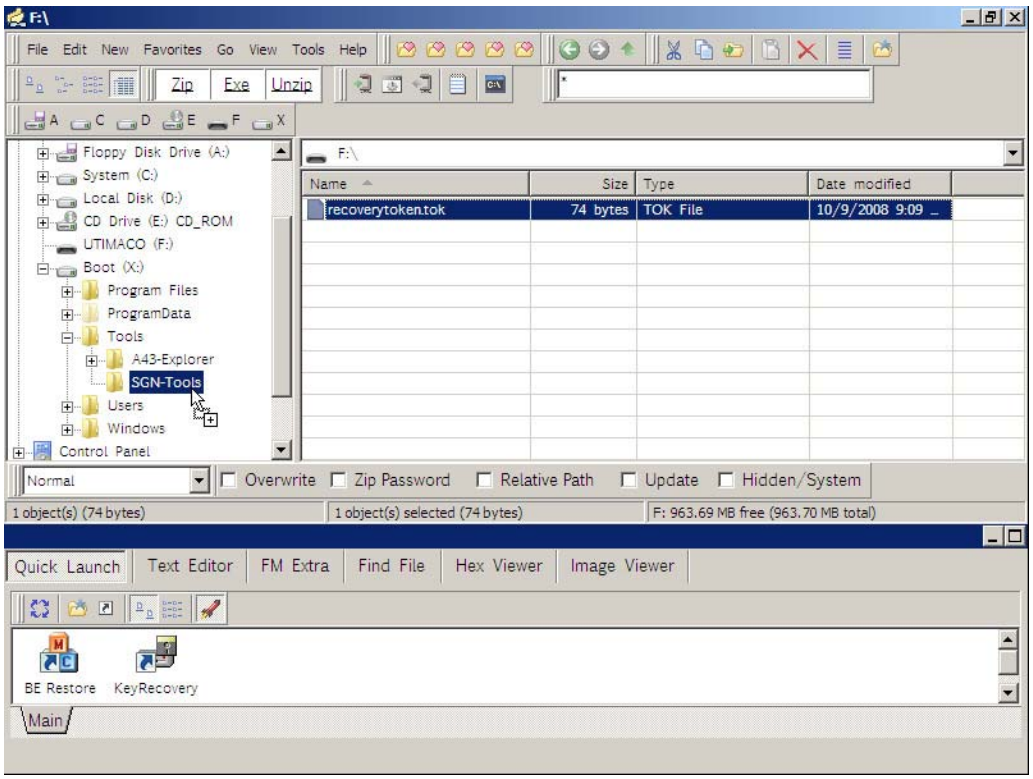
23.9.3 Virtuellen Client in das KeyRecovery Tool importieren

Voraussetzung:

- Der Computer wurde von der Recovery Disk gebootet.
- Stellen Sie sicher, dass das USB-Laufwerk mit der Datei recoverytoken.tok erfolgreich bereitgestellt wurde.

1. Wählen Sie im Windows PE Dateimanager das Laufwerk aus, auf dem der virtuelle Client gespeichert ist. Die Datei recoverytoken.tok wird auf der rechten Seite angezeigt.

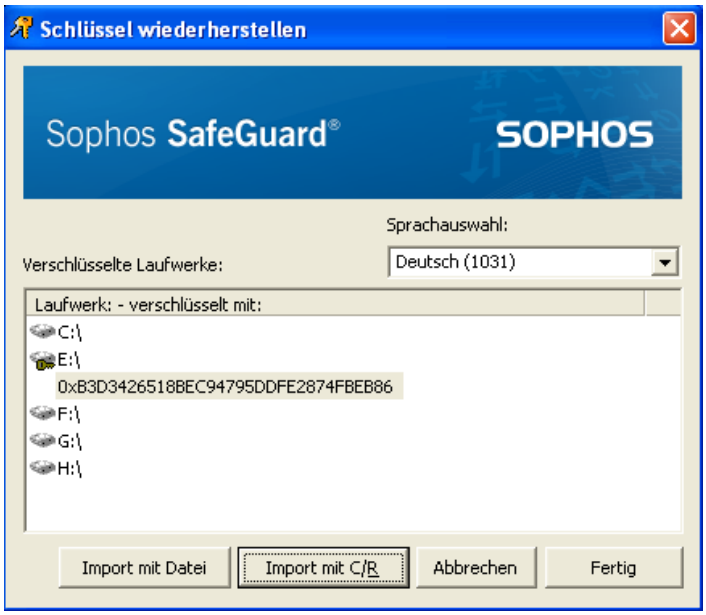
2. Wählen Sie die Datei recoverytoken.tok aus und ziehen Sie sie auf das Laufwerk, auf dem sich das KeyRecovery Tool befindet. Legen Sie die Datei hier im Verzeichnis Tools\SGN-Tools ab.



23.9.4 Challenge im KeyRecovery Tool starten

1. Klicken Sie unten im Bereich **Quick Launch** des Dateimanagers auf das KeyRecovery-Symbol, um das KeyRecovery Tool zu öffnen. Das Key Recovery Tool zeigt die Schlüssel-ID verschlüsselter Laufwerke.

Das Tool startet und zeigt eine Liste aller Volumes mit den jeweiligen Verschlüsselungsinformationen (Schlüssel-ID).



2. Wählen Sie das Volume, das Sie entschlüsseln möchten und klicken Sie auf Import mit C/R, um den Challenge-Code zu erzeugen.

Die Datei mit dem virtuellen Client wird als Referenz in der SafeGuard Enterprise Datenbank verwendet und in der Challenge angegeben. Der Challenge-Code wird erzeugt und angezeigt.

3. Übermitteln Sie den Namen des virtuellen Clients und den Challenge-Code an den Helpdesk, z. B. über Telefon oder eine Textmitteilung. Hierzu steht eine Buchstabierhilfe zur Verfügung.

23.9.5 Response mit virtuellen Clients erzeugen

Um auf einen durch SafeGuard Enterprise geschützten Computer zuzugreifen und eine Response mit virtuellen Clients zu erzeugen, sind zwei Aktionen erforderlich:

1. Bestätigen Sie den virtuellen Client in der SafeGuard Management Center Datenbank.
2. Wählen Sie die erforderliche Recovery-Aktion aus:
   - Die Challenge kann zum Wiederherstellen eines einzelnen Schlüssels für den Zugriff auf ein verschlüsseltes Volume auf einem Computer, der mit dem SafeGuard Enterprise Server verbunden ist, gestartet werden. Wählen Sie **Schlüssel angefordert Recovery-Schlüssel aus der Datenbank**.
   - Die Challenge kann zum Wiederherstellen eines einzelnen Schlüssels für den Zugriff auf ein verschlüsseltes Volume auf einem Standalone-Computer gestartet werden, der nie eine Verbindung zum SafeGuard Enterprise Server hat. Wählen Sie **Schlüssel angefordert Schlüssel-Recovery-Datei (Standalone)**.
   - Die Challenge kann zum Wiederherstellen mehrerer Schlüssel für den Zugriff auf verschlüsselte Volumes auf einem Computer, der mit dem SafeGuard Enterprise Server verbunden ist. Die Schlüssel werden in einer Datei gespeichert, die mit einem Zufallskennwort verschlüsselt wird, das in der Datenbank abgelegt ist. Das Kennwort ist für jede erstellte Schlüsseldatei einzigartig. Das Kennwort wird innerhalb des Response-Codes an den Zielcomputer übertragen. Wählen Sie **Schlüssel angefordert**

23.9.6 Virtuellen Client bestätigen

Der virtuelle Client muss im SafeGuard Management Center unter **Virtuelle Clients** angelegt worden sein und er muss in der Datenbank zur Verfügung stehen.

1. Klicken Sie im SafeGuard Management Center auf **Extras** > **Recovery**, um den Recovery-Assistenten zu öffnen.
2. Wählen Sie unter **Recovery-Typ** die Option **Virtueller Client**.

3. Geben Sie den Namen des virtuellen Client ein, den Sie vom Benutzer erhalten haben. Hierzu gibt es verschiedene Möglichkeiten:
   - Geben Sie den eindeutigen Namen direkt ein.
   - Wählen Sie einen Namen, indem Sie auf **[...]** im Abschnitt **Virtueller Client** des Dialogs **Recovery-Typ** klicken. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit virtuellen Clients wird angezeigt. Wählen Sie den gewünschten virtuellen Client aus und klicken Sie auf **OK**. Der Name des virtuellen Clients wird nun im Fenster **Recovery-Typ** unter **Virtueller Client** angezeigt.
4. Klicken Sie auf **Weiter**, um den Namen der Datei mit dem virtuellen Client zu bestätigen.

Im nächsten Schritte wählen Sie die erforderliche Recovery-Aktion aus.

23.9.7 Angeforderten Schlüssel auswählen (zentral verwaltete Clients)

Voraussetzung:

Sie müssen den erforderlichen virtuellen Client im Recovery-Assistenten des SafeGuard Management Center ausgewählt haben.

Eine Response kann nur für zugewiesene Schlüssel erzeugt werden. Ist ein Schlüssel inaktiv, d. h. der Schlüssel ist nicht mindestens einem Benutzer zugewiesen, ist eine Response mit einem virtuellen Client nicht möglich. In diesem Fall kann der inaktive Schlüssel zunächst einem beliebigen Benutzer zugewiesen werden. Danach kann eine Response für den Schlüssel generiert werden.

1. Wählen Sie im Recovery-Assistenten unter Virtueller Client die erforderliche Recovery-Aktion **Schlüssel angefordert** und klicken Sie auf **Weiter**.
2. Aktivieren Sie **Recovery-Schlüssel aus der Datenbank auswählen**.
3. Klicken Sie auf **[...]**. Sie können sich die Schlüssel entweder nach Schlüssel-ID oder symbolischem Namen anzeigen lassen. Klicken Sie auf **Suchen**, wählen Sie den Schlüssel und klicken Sie auf **OK**.
4. Bestätigen Sie Ihre Auswahl mit **Weiter**. Das Fenster für die Eingabe des Challenge-Codes wird angezeigt.
5. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

Wenn der Challenge-Code korrekt eingegeben wurde, wird der Response-Code erzeugt. Wurde der Code nicht korrekt eingegeben, so wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.

6. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der angeforderte Schlüssel wird innerhalb des Response-Codes an die Benutzerumgebung übertragen.

23.9.8 Schlüssel-Recovery-Datei auswählen (Standalone-Computer)

Sie müssen den erforderlichen virtuellen Client im Recovery-Assistenten des SafeGuard Management Center ausgewählt haben.

Die Schlüssel-Recovery-Datei, die zur Wiederherstellung des Zugriffs auf den Computer erforderlich ist, muss dem Helpdesk zur Verfügung stehen, z. B. über eine Netzwerkfreigabe.

1. Wählen Sie im Recovery-Assistenten unter Virtueller Client die erforderliche Recovery-Aktion **Schlüssel angefordert** und klicken Sie auf **Weiter**.
2. Aktivieren Sie die Option **Schlüssel-Recovery-Datei mit Recovery-Schlüssel auswählen**.
3. Klicken Sie neben dieser Option auf **[...]**, um nach der entsprechenden Datei zu suchen. Zur Vereinfachung tragen die Recovery-Dateien den Namen des jeweiligen Computers: computername.GUID.xml.
4. Bestätigen Sie Ihre Auswahl mit **Weiter**. Das Fenster für die Eingabe des Challenge-Codes wird angezeigt.
5. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

Wenn der Challenge-Code korrekt eingegeben wurde, wird der Response-Code erzeugt. Wurde der Code nicht korrekt eingegeben, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.

6. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der angeforderte Schlüssel wird mit dem Response-Code an die Benutzerumgebung übertragen.

23.9.9 Mehrere Schlüssel in einer Schlüsseldatei auswählen

Sie müssen die erforderliche Datei mit dem virtuellen Client im SafeGuard Management Center Recovery-Assistenten ausgewählt haben.

Sie müssen die Schlüsseldatei zuvor im SafeGuard Management Center unter **Schlüssel & Zertifikate** angelegt haben und das Kennwort, mit dem die Datei verschlüsselt ist, muss in der Datenbank gespeichert sein.

1. Wählen Sie im Recovery-Assistenten unter Virtueller Client die erforderliche Recovery-Aktion **Kennwort für ausgewählte Schlüsseldatei** und klicken Sie auf **Weiter**.
2. Klicken Sie neben dieser Option auf **[...]** und dann auf **Suchen**. Wählen Sie die Schlüsseldatei aus und klicken Sie auf **OK**.
3. Bestätigen Sie Ihre Auswahl mit **Weiter**. Das Fenster für die Eingabe des Challenge-Codes wird angezeigt.
4. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

Wenn der Challenge-Code korrekt eingegeben wurde, wird der Response-Code erzeugt. Wurde der Code nicht korrekt eingegeben, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.

5. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

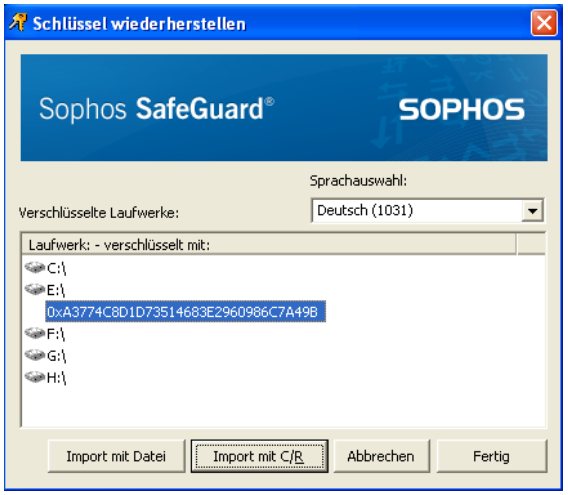
Der angeforderte Schlüssel wird mit dem Response-Code an die Benutzerumgebung übertragen.

23.9.10 Response-Code im KeyRecovery Tool eingeben

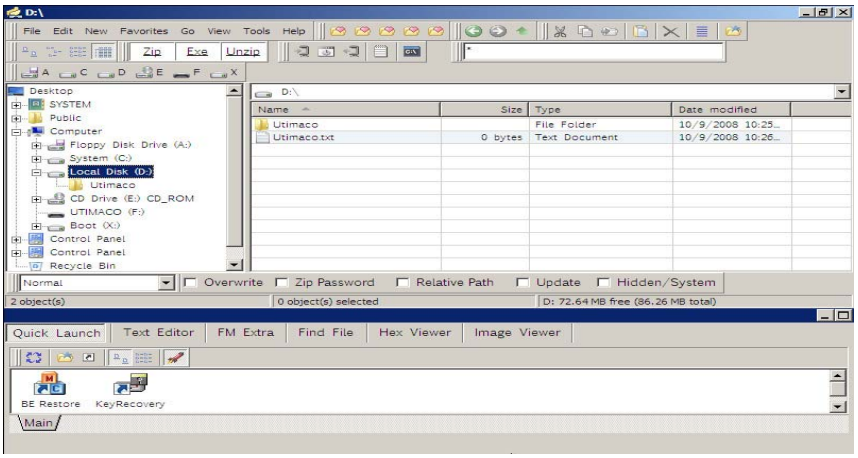
1. Geben Sie im KeyRecovery Tool auf dem Endpoint-Computer den Response-Code ein, den Sie vom Helpdesk erhalten haben.

   Mit dem Response-Code wird der erforderliche Recovery-Schlüssel übertragen.

2. Klicken Sie auf **OK**. Das für das Challenge/Response-Verfahren gewählte Laufwerk wird entschlüsselt.



3. Um sicherzustellen, dass die Entschlüsselung erfolgreich durchgeführt werden konnte, wählen Sie das entschlüsselte Laufwerk im Windows PE Dateimanager aus:



Der Inhalt des entschlüsselten Laufwerks wird nun im Dateimanager angezeigt. Das Dateisystem und die Kapazität sowie der benutzte/freie Speicherplatz werden nun in den Eigenschaften des entschlüsselten Laufwerks angegeben.

Der Zugriff auf die in dieser Partition gespeicherten Daten ist wiederhergestellt. Nach der erfolgreichen Entschlüsselung haben Sie auf dem entsprechenden Laufwerk Lese- und Schreibzugriff für Daten. Sie können Daten vom und auf das Laufwerk kopieren.

23.10 Challenge/Response für Sophos SafeGuard Clients (Standalone)

SafeGuard Enterprise bietet auch ein Challenge/Response-Verfahren für Standalone-Computer (Sophos SafeGuard Clients). Diese Computer haben nie eine Verbindung zum SafeGuard Enterprise Server, auch nicht vorübergehend. Sie werden im Standalone-Modus betrieben. Da sie nicht in der SafeGuard Enterprise Datenbank registriert sind, stehen keine Informationen für ihre Identifikation, die für ein Challenge/Response-Verfahren benötigt werden, zur Verfügung.

Für diese Computer bietet SafeGuard Enterprise ein Challenge-Response-Verfahren, z. B. für den Fall, dass ein Benutzer sein Kennwort vergessen oder zu oft falsch eingegeben hat. Die für das Challenge/Response-Verfahren benötigten Identifikationsinformationen basieren in diesem Fall auf der Schlüssel-Recovery-Datei. Diese Schlüssel-Recovery-Datei wird auf jedem Endpoint-Computer während der Installation der SafeGuard Enterprise Verschlüsselungssoftware erzeugt.

Steht diese Schlüssel-Recovery-Datei dem Helpdesk zur Verfügung, z. B. über eine Netzwerkfreigabe, so kann ein Challenge/Response-Verfahren für den durch SafeGuard Enteprise geschützten Computer durchgeführt werden.

Um die Suche nach und die Gruppierung von Recovery-Dateien zu vereinfachen, enthalten die Dateienamen den Namen des Computers: computername.GUID.xml. Somit sind Suchvorgänge mit Asterisken (*) als Platzhalter möglich, z. B.: *.GUID.xml.

Hinweis: Wenn ein Computer umbenannt wird, wird er im Local Cache nicht automatisch entsprechend umbenannt. Im Local Cache werden alle Schlüssel, Richtlinien, Benutzertifikate und Audit-Dateien gespeichert. Für die Datei-Generierung muss der neue Computername daher aus dem Local Cache entfernt werden, so dass nur der vorige Name verbleibt, auch wenn der Computer unter Windows umbenannt werden.

23.10.1 Recovery-Aktionen für Sophos SafeGuard Clients (Standalone)

Für einen Endpoint-Computer kann in den folgenden Situationen ein Challenge/Response-Verfahren gestartet werden:

- Der Benutzer hat sein Kennwort auf POA-Ebene zu oft falsch eingegeben und der Computer wurde gesperrt.
- Der Benutzer hat das Kennwort vergessen.
- Ein beschädigter Local Cache muss repariert werden.

Für einen Standalone-Computer steht kein Benutzerschlüssel in der Datenbank zur Verfügung. Somit ist in einem Challenge/Response-Verfahren nur die Recovery-Aktion **SGN Client ohne Benutzeranmeldung booten**.

Das Challenge/Response-Verfahrens ermöglicht das Booten des Computers durch die Power-on Authentication. Der Benutzer kann sich dann an Windows anmelden.

Der Benutzer hat das Kennwort auf POA-Ebene zu oft falsch eingegeben und der Computer wurde gesperrt.

Der Computer ist gesperrt und der Benutzer wird dazu aufgefordert, ein Challenge/Response-Verfahren zu starten, um wieder Zugriff auf den Computer zu erhalten. Da in diesem Fall das Kennwort nicht zurückgesetzt werden muss, weil der Benutzer das Kennwort noch weiß, ermöglicht das Challenge/Response-Verfahren das Booten des Computers durch die Power-on Authentication. Der Benutzer kann dann das korrekte Kennwort auf Windows-Ebene eingeben und den Computer wieder benutzen.

Der Benutzer hat das Kennwort vergessen

Hinweis: Wir empfehlen, in erster Linie Local Self Help einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Mit Recovery über Local Self Help kann sich der Benutzer selbst das aktuelle Benutzerkennwort unter Wahrung der Vertraulichkeit in der Power-on Authentication anzeigen lassen und es weiterhin zur Anmeldung verwenden. Für weitere Informationen siehe *Recovery über Local Self Help*, Seite 4.

Wenn das Kennwort über ein Challenge/Response-Verfahren wiederhergestellt wird, muss das Kennwort zurückgesetzt werden.

1. Das Challenge/Response-Verfahren ermöglicht das Booten des Computers durch die Power-on Authentication.
2. Da dem Benutzer das Kennwort nicht bekannt ist, kann er es im Windows-Dialog nicht eingeben. Das Kennwort muss daher auf Windows-Ebene zurückgesetzt werden. Hierzu sind weitere Recovery-Vorgänge außerhalb von SafeGuard Enterprise erforderlich, die über Windows-Standard-Verfahren durchgeführt werden müssen.

Hinweis: Wir empfehlen, das Kennwort vor dem Challenge/Response-Verfahren nicht zentral im Active Directory zurückzusetzen. Dadurch wird sichergestellt, dass das Kennwort zwischen Windows und SafeGuard Enterprise synchron bleibt. Stellen Sie sicher, dass der Windows-Helpdesk entsprechend informiert ist.

3. Wir empfehlen, die folgenden Methoden für das Zurücksetzen des Kennworts auf Windows-Ebene:
   - Über ein Service-Benutzerkonto oder ein Administratorkonto mit den erforderlichen Windows-Rechten auf dem Endpoint-Computer
   - Über eine Windows-Kennwortrücksetz-Diskette auf dem Endpoint-Computer

     Als Helpdesk-Beauftragter können Sie den Benutzer darüber informieren, welche Methode benutzt werden soll, und ihm die zusätzlichen Windows-Anmeldeinformationen oder die erforderliche Diskette zur Verfügung stellen.
4. Der Benutzer gibt das vom Helpdesk zur Verfügung gestellte neue Kennwort auf Windows-Ebene ein. Unmittelbar danach ändert der Benutzer das Kennwort in ein nur ihm bekanntes Kennwort.
5. SafeGuard Enterprise stellt fest, dass das neu gewählte Kennwort nicht mehr den aktuellen Kennwort entspricht, das in der POA verwendet wird. Der Benutzer wird aufgefordert, das alte Kennwort einzugeben. Da er das Passwort vergessen hat, muss er auf **Abbrechen** klicken.
6. Da beim Zurücksetzen eines Kennworts ohne Angabe des alten Kennworts in SafeGuard Enterprise ein neues Zertifikat generiert werden muss, muss der Benutzer diesen Vorgang bestätigen.
7. Ein neues Benutzerzertifikat wird basierend auf dem neu gewählten Windows-Kennwort erstellt. Dies ermöglicht es dem Benutzer, sich wieder an seinem Computer und an der Power-on Authentication mit dem neuen Kennwort anzumelden.

Schlüssel für SafeGuard Data Exchange

Hinweis: Wenn der Benutzer das Windows-Kennwort vergessen hat und ein neues eingeben muss, wird auch ein neues Zertifikat erstellt. In diesem Fall kann der Benutzer daher nicht mehr die bereits für SafeGuard Data Exchange erstellten Schlüssel verwenden. Damit bereits für SafeGuard Data Exchange generierte Benutzerschlüssel weiterhin verwendet werden können, müssen dem Benutzer die SafeGuard Data Exchange Passphrasen zur Reaktivierung dieser Schlüssel bekannt sein.

23.10.2 Response für Standalone-Computer mit der Schlüssel-Recovery-Datei erzeugen

Hinweis: Die Schlüssel-Recovery-Datei, die während der Installation der SafeGuard Enterprise Verschlüsselungssoftware generiert wurde, muss an einem Speicherort abgelegt sein, auf den der Helpdesk-Beauftragte Zugriff hat. Darüber hinaus muss der Name der Datei bekannt sein.

So generieren Sie eine Response:

1. Wählen Sie in der Menüleiste des SafeGuard Management Center **Extras > Recovery** , um den Recovery-Assistenten zu öffnen.
2. Wählen Sie unter **Recovery-Typ** die Option **Sophos SafeGuard Client (Standalone)**.
3. Klicken Sie auf **Browse**, um die erforderliche Schlüssel-Recovery-Datei auszuwählen. Zur Vereinfachung der Identifizierung tragen die Recovery-Dateien den Namen des Computers: computername.GUID.xml.
4. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

Wenn der Challenge-Code korrekt eingegeben wurde, werden die vom Endpoint-Computer angeforderte Recovery-Aktion sowie die möglichen Recovery-Aktionen angezeigt. Wenn der Code nicht korrekt eingegeben wurde, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.

5. Wählen Sie die vom Benutzer durchzuführende Aktion aus und klicken Sie auf **Weiter**.
6. Es wird ein Response-Code erzeugt. Teilen Sie den Response-Code dem Benutzer mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der Benutzer kann den Response-Code eingeben, die angeforderte Aktion ausführen und dann wieder mit dem Computer arbeiten.

24 Systemwiederherstellung

SafeGuard Enterprise verschlüsselt Dateien und Laufwerke transparent. Darüber hinaus können auch Bootlaufwerke verschlüsselt werden, so dass Entschlüsselungsfunktionalitäten wie Code, Verschlüsselungsalgorithmen und Verschlüsselungschlüssel sehr früh in der Bootphase verfügbar sein müssen. Folglich kann auf verschlüsselte Informationen nicht zugegriffen werden, wenn entscheidende SafeGuard Enterprise Module nicht verfügbar sind oder nicht funktionieren.

Die folgenden Abschnitte beschreiben mögliche Fehlerquellen und Recovery-Verfahren.

24.1 Daten-Recovery durch Booten von einem externen Medium

Dieser Recovery-Typ kann angewendet werden, wenn sich der Benutzer zwar noch an der POA anmelden, jedoch nicht mehr auf das verschlüsselte Volume zugreifen kann. In diesem Fall kann der Zugriff auf die verschlüsselten Daten durch Booten des Computers über eine für SafeGuard Enterprise angepasste Windows PE Recovery Disk wiederhergestellt werden.

Voraussetzungen:

- Der Benutzer, der vom externen Medium bootet, muss dazu berechtigt sein. Dieses Recht kann entweder im SafeGuard Management Center innerhalb einer Richtlinie vom Typ **Authentisierung** konfiguriert werden (**Benutzer darf Volume entschlüsseln** auf **Ja** eingestellt), oder es kann für die einmalige Benutzung über ein Challenge/Response-Verfahren erlangt werden.
- Der Computer muss das Booten von anderen Medien außer von der fest eingebauten Festplatte unterstützen.

So erhalten Sie wieder Zugriff auf die verschlüsselten Daten auf dem Computer:

1. Sie erhalten die SafeGuard Enterprise Recovery Disk vom technischen Support.

   Für den Helpdesk steht die Windows PE Recovery Disk mit den aktuellen SafeGuard Enterprise Filtertreibern auf der Sophos Support-Website zum Download zur Verfügung. Weitere Informationen finden Sie in unserer Wissensdatenbank: http://www.sophos.com/support/knowledgebase/article/108805.html.

2. Melden Sie sich an der Power-on Authentication mit Ihren Anmeldeinformationen an.

3. Legen Sie die Windows PE Recovery Disk ein.
4. Wählen Sie im POA-Anmeldedialog unter **Weiterbooten von:** die Option **externes Medium**.Der Computer wird gestartet.

Der Zugriff auf die auf dieser Partition gespeicherten Daten ist wiederhergestellt.

24.2 Beschädigter MBR

Zur Problembehebung im Fall eines beschädigten MBR bietet SafeGuard Enterprise das Tool BE_Restore.exe.

Eine detaillierte Beschreibung zur Wiederherstellung eines beschädigten MBR finden Sie in der SafeGuard Tools-Anleitung unter BE_Restore.exe.

24.3 Code

Es kann auf eine Festplatte mit einem beschädigten Kernel-Bootcode zugegriffen werden. Denn Schlüssel werden getrennt vom Kernel in der so genannten KSA (Key Storage Area) gespeichert. Durch die Trennung von Kernel und Schlüsseln können solche Laufwerke angeschlossen an einen anderen Computer entschlüsselt werden.

Dazu benötigt der Benutzer, der sich an dem anderen Computer anmeldet, einen Schlüssel der KSA der nicht bootbaren Partition in seinem Schlüsselring.

Im schlimmsten Fall ist die Partition nur mit dem Boot_Key des anderen Computers verschlüsselt. In diesem Fall muss der Haupt-Sicherheitsbeauftragte oder der Recovery-Beauftragte dem Benutzer diesen Boot_Key zuweisen.

Für eine detaillierte Beschreibung dieses Vorgangs, voir *„Slaven“ einer Festplatte*, à la page 275.

24.4 Volumes

SafeGuard Enterprise bietet die laufwerksbezogene Verschlüsselung. Dies beinhaltet die Speicherung von Verschlüsselungsinformationen bestehend aus Bootsektor, primäre bzw. Backup-KSA und Originalbootsektor auf jedem Laufwerk selbst.

Sobald eine dieser Einheiten beschädigt ist, besteht kein Zugriff mehr auf das Volume:

- eine der beiden Key Storage Areas (KSA)
- Original-MBR

24.4.1 Bootsektor

Der Bootsektor eines Volumes wird bei der Verschlüsselung gegen den SafeGuard Enterprise Bootsektor ausgetauscht.

Der SafeGuard Enterprise Bootsektor enthält Informationen über

- den Ort der primären und Backup-KSA in Clustern und Sektoren bezogen auf den Start der Partition
- die Größe der KSA

Auch wenn der SafeGuard Enterprise Bootsektor zerstört ist, ist kein Zugriff auf verschlüsselte Volumes möglich.

Das Tool BE_Restore kann den zerstörten Bootsektor wiederherstellen. Eine detaillierte Beschreibung dieses Tools finden Sie in der SafeGuard Tools-Anleitung.

24.4.2 Originaler Bootsektor

Beide KSAs enthalten den originalen Bootsektor. Das ist jener, der ausgeführt wird, nachdem der DEK (Data Encryption Key) entschlüsselt wurde und der Algorithmus und der Schlüssel in den BE Filtertreiber geladen wurden.

Ist dieser Bootsektor defekt, kann Windows nicht auf das Volume zugreifen. Normalerweise wird die bekannte Fehlermeldung „Gerät ist nicht formatiert. Möchten Sie es jetzt formatieren? Ja/Nein“ angezeigt.

SafeGuard Enterprise wird den DEK für dieses Volume dennoch laden. Jedes Tool, das den Bootsektor reparieren kann, soll dennoch laufen - vorausgesetzt, es passiert den SafeGuard Enterprise Upper Volume Filter.

24.5 Windows Bootprobleme

SafeGuard Enterprise ist mit seinem kryptographischen Konzept der volume-spezifischen Schlüssel (Bootsektor, Key Storage Area KSA) sehr flexibel.

Sie können ein beschädigtes System durch Booten eines Wiederherstellungsmediums von der Power-on Authentication von SafeGuard Enterprise aus (Windows PE mit dem SafeGuard Enterprise Verschlüsselungs-Subsystem installiert) retten. Diese Medien haben einen transparenten Ver-/Entschlüsselungszugriff auf mit SafeGuard Enterprise verschlüsselte Volumes. Der Grund für das nicht bootbare System kann von dort aus beseitigt werden.

24.5.1 Verschlüsselungs-Subsystem

Verschlüsselungs-Subsysteme sind z. B. BEFLT.sys Systeme. Führen Sie das unter Windows Bootprobleme beschriebene Verfahren aus und reparieren Sie das System.

24.5.2 GINA-Probleme

Führen Sie zur Behebung von GINA-Problemen, z. B. Circular Loops, das unter Windows Bootprobleme beschriebene Verfahren aus.

24.6 Setup WinPE für SafeGuard Enterprise

Um Zugriff auf verschlüsselte Laufwerke mit dem BOOTKEY eines Computers innerhalb einer WinPE Umgebung zu erhalten, stellt SafeGuard Enterprise WinPE mit notwendigen SafeGuard Enterprise Funktionsmodulen wie Treibern zur Verfügung. Um SetupWinPE zu starten, geben Sie folgenden Befehl ein:

SetupWinPE -pe2 <WinPE Image-Datei>

WinPE Image-Datei ist dabei die vollständige Pfadangabe des I386 Verzeichnisses für eine WinPE-CD.

SetupWinPE führt alle erforderlichen Änderungen durch.

Remarque: Beachten Sie, dass über eine derartige WinPE-Umgebung nur auf verschlüsselte Laufwerke zugegriffen werden kann, die mit dem BOOTKEY verschlüsselt sind. Auf Laufwerke, die mit einem Benutzerschlüssel verschlüsselt sind, kann nicht zugegriffen werden, da die Schlüssel in dieser Umgebung nicht verfügbar sind.

24.7 „Slaven“ einer Festplatte

SafeGuard Enterprise erlaubt das Slaven von verschlüsselten Volumes oder Festplatten. Es gestattet dem Endbenutzer, dem Windows-Administrator, dem SafeGuard Enterprise Sicherheitsbeauftragten trotz sektorbasierter Verschlüsselung neue Volumes oder Festplatten anzuschließen oder zu entfernen.

Die Key Storage Area (KSA) eines Volumes enthält selbst alle notwendigen Informationen:

- Den zufallsgenerierten DEK (Data Encryption Key)
- Eine Identifikation für den Verschlüsselungsalgorithmus, mit dem das Volume verschlüsselt ist.

- Die Liste von GUIDs der KEKs (Key Encryption Keys), die den DEK verschlüsseln und entschlüsseln können.
- Das Volume selbst enthält seine Größe.

Auf ein mit SafeGuard Enterprise verschlüsseltes Volume kann von allen SafeGuard Enterprise Endpoint-Computern zugegriffen werden, vorausgesetzt der Benutzer oder der Computer besitzt einen KEK des KSA des Volumes im Schlüsselring.

Benutzer oder Computer müssen den durch den KEK verschlüsselten DEK entschlüsseln können.

Auf ein Volume, das mit einem verteilbaren KEK, wie einem OU-, Gruppen- oder Domänenschlüssel verschlüsselt ist, kann von vielen Benutzern und Computern zugegriffen werden, da viele Benutzer/Computer einer Domäne diesen Schlüssel in ihrem Schlüsselring haben.

Jedoch kann auf ein Volume, das nur mit dem individuellen Bootschlüssel ("Boot_machinename") des SafeGuard Enterprise Clients verschlüsselt wird, nur von diesem Computer selbst zugegriffen werden.

Soll ein Volume nicht in seinem originalen Computer booten, kann es in einem anderen SafeGuard Enterprise Client „geslaved" werden. Dann kann aber auf den korrekten Bootschlüssel nicht zugegriffen werden. Der Zugriff darauf muss möglich gemacht werden.

Immer wenn der Benutzer versucht, von einem anderen Computer auf das Volume zuzugreifen, ist dies möglich, weil jetzt erneut Übereinstimmung zwischen den KEKs im KSA und den Schlüsselringen der anderen Benutzer oder Computer besteht.

24.7.1 Beispiel

Alice besitzt ihren individuellen Benutzerschlüssel. Immer, wenn sie sich an ihrem anderen Computer anmeldet ("Laptop_Alice"), hat sie keinen Zugriff auf das Volume, das mit dem Bootschlüssel des Computers "SGNCLT" verschlüsselt ist.

Der SafeGuard Enterprise Client "SGMCLT" besitzt nur seinen eigenen Bootschlüssel BOOT_SGMCLT.

Der Sicherheitsbeauftragte teilt Alice den Bootschlüssel “BOOT_SGNCLT” auf folgende Weise zu:

1. Auswahl des Benutzers Alice
2. Klick auf das „Fernglas“-Symbol in der SafeGuard Enterprise Symbolleiste. Das startet den Suchdialog, in dem auch Bootschlüssel angezeigt werden können.
3. Auswahl des Schlüssels “BOOT_SGMCLT”.

Jetzt verfügt Alice über zwei Schlüssel – „User_Alice“ und „BOOT_SGMCLT“. Das kann unter **Schlüssel & Zertifikate** nachgeprüft werden.

Der Schlüssel “BOOT_SGMCLT” ist zweimal zugewiesen – zum Computer SGMCLT und zum Benutzer Alice.

Alice ist es nun möglich, auf das verschlüsselte Volume von jedem anderen SafeGuard Enterprise Client zuzugreifen, auf dem sie sich anmelden kann.

Dann kann sie auf einfache Weise Tools, wie den Windows Explorer oder regedit.exe, verwenden, um die Ursache des Bootproblems zu beseitigen.

Wenn im schlimmsten Fall das Problem nicht gelöst werden kann, kann sie Daten auf ein anderes Laufwerk sichern, das Volume neu formatieren oder es ganz neu aufsetzen.

25 Bestand- und Statusinformationen

SafeGuard Enterprise liest eine Fülle von Bestand- und Statusinformationen von den Clients aus. Diese Informationen zeigen den aktuell bekannten globalen Zustand der einzelnen Maschinen. Im SafeGuard Management Center werden diese Informationen im Bereich **Benutzer & Computer** in der Registerkarte **Bestand** übersichtlich dargestellt.

Als Sicherheitsbeauftragter können Sie die im SafeGuard Management Center angezeigten Bestand- und Statusinformationen einsehen und ausdrucken. So lassen sich zum Beispiel zum Nachweis der Verschlüsselung von Endgeräten die entsprechenden ausgedruckten Berichte erstellen. Umfassende Sortier- und Filterfunktionen unterstützen Sie bei der Auswahl der relevanten Informationen.

Der **Bestand** liefert u. a. folgende Informationen zu den einzelnen Maschinen:

- Informationen zu erhaltenen Richtlinien
- Informationen zum Verschlüsselungsstatus
- Informationen zum POA-Status sowie zum POA-Typ
- Informationen zu den installierten SafeGuard Enterprise Modulen
- Informationen zum WOL-Status
- Benutzerinformationen

25.1 Bestandinformationen einsehen

So rufen Sie die Bestandinformationen ab:

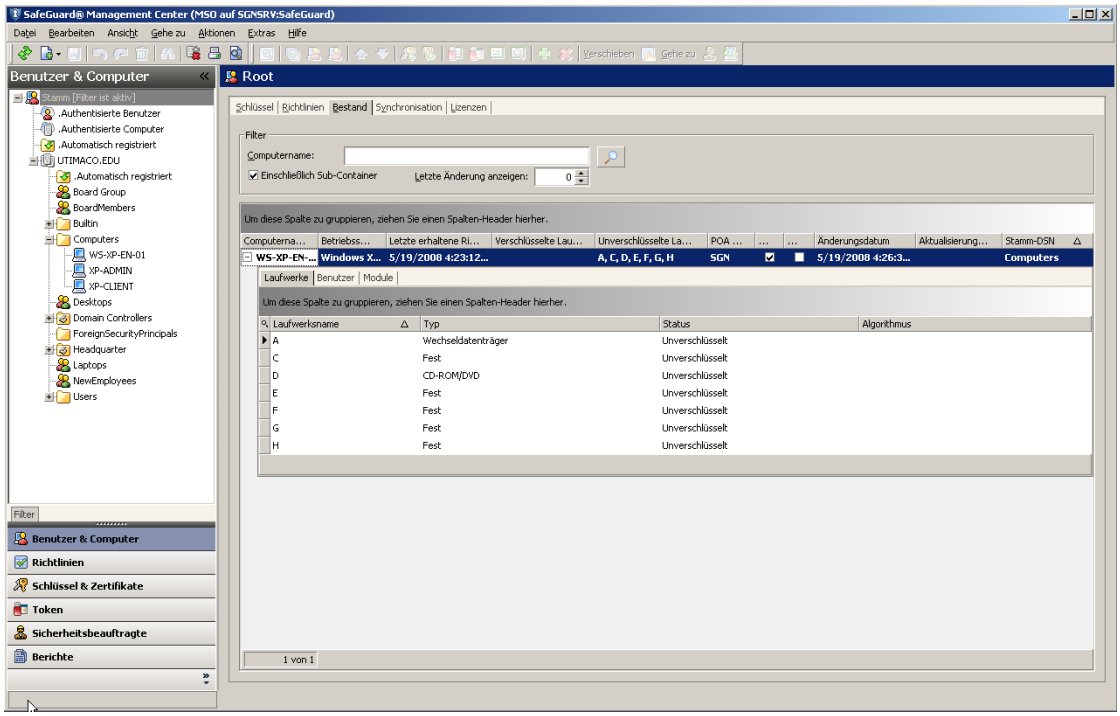
Sie befinden sich im geöffneten Management Center.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Centers auf die Schaltfläche **Benutzer & Computer**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf den jeweiligen Container (Domäne, Arbeitsgruppe oder Computer).
3. Wechseln Sie im Aktionsbereich auf der rechten Seite in die Registerkarte **Bestand**.
4. Wählen Sie im Bereich **Filter** die gewünschten Filter für die Bestandsanzeige, siehe *Bestandinformationen filtern* auf Seite 280.

Hinweis: Wenn Sie einen einzelnen Computer wählen, stehen die Bestandinformationen direkt nach dem Wechsel in die Registerkarte **Bestand** zur Verfügung. Der Bereich **Filter** ist hier nicht verfügbar.

5. Klicken Sie im Bereich **Filter** auf das Lupensymbol.

Die Bestand- und Statusinformationen werden in einer Übersichtstabelle für alle Maschinen des ausgewählten Containers angezeigt. Darüber hinaus stehen für die einzelnen Maschinen die Registerkarten **Laufwerke**, **Benutzer** und **Merkmale** zur Verfügung.

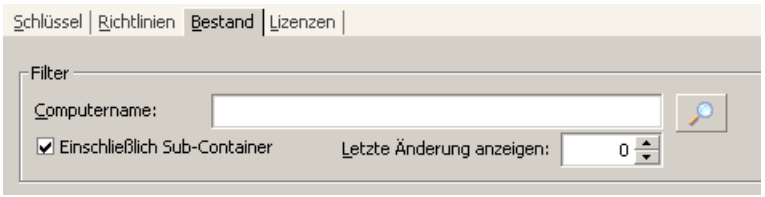

SafeGuard® Management Center (MSO auf SGNSRV:SafeGuard)
Datei Bearbeiten Ansicht Gehe zu Aktionen Extras Hilfe
Benutzer & Computer
Root
Schlüssel Richtlinien Bestand Synchronisation Lizenzen
Filter
Computername:
Einschließlich Sub-Container
Letzte Änderung anzeigen:
Um diese Spalte zu gruppieren, ziehen Sie einen Spalten-Header hierher.
Computerna... Betriebss... Letzte erhaltene Ri... Verschlüsselte Lau... Unverschlüsselte La... POA ... Änderungsdatum Aktualisierung... Stamm-DSN
WS-XP-EN-... Windows X... 5/19/2008 4:23:12... A, C, D, E, F, G, H SGN 5/19/2008 4:26:3... Computers
Laufwerke Benutzer Module
Um diese Spalte zu gruppieren, ziehen Sie einen Spalten-Header hierher.
Laufwerksname Typ Status Algorithmus
A Wechseldatenträger Unverschlüsselt
C Fest Unverschlüsselt
D CD-ROM/DVD Unverschlüsselt
E Fest Unverschlüsselt
F Fest Unverschlüsselt
G Fest Unverschlüsselt
H Fest Unverschlüsselt
1 von 1
Filter
Benutzer & Computer
Richtlinien
Schlüssel & Zertifikate
Token
Sicherheitsbeauftragte
Berichte

Durch Klicken auf die einzelnen Spalten-Header lassen sich die Bestand- und Statusinformationen nach den jeweiligen Spalteninformationen sortieren. Darüber hinaus steht über das Kontextmenü der einzelnen Spalten eine Reihe von Funktionen für die Sortierung, Gruppierung und Anpassung der angezeigten Anzeige zur Verfügung.

25.1.1 Bestandinformationen filtern

Für die Übersicht der Bestandinformationen für OUs lassen sich Filter definieren, um die Darstellung nach bestimmten Kriterien einzuschränken.

Im **Filter**-Bereich der Registerkarte **Bestand** stehen folgende Felder für die Definition von Filtern zur Verfügung:



Feld	Beschreibung
Computername	Um die Bestand- und Statusinformationen für bestimmte Computer anzeigen zu lassen, geben Sie in diesem Feld den Computernamen an.
Einschließlich Sub-Container	Aktivieren Sie dieses Feld, um Sub-Container in die Anzeige mit einzubeziehen.
Letzte Änderung anzeigen	Legen Sie in diesem Feld die Anzahl der anzuzeigenden letzten Änderungen festlegen.

Darüber hinaus können Sie mit dem Filter-Editor benutzerdefinierte Filter erstellen. Der Filter-Editor lässt sich über das Kontextmenü der einzelnen Berichtsspalten aufrufen. Im Fenster **Filterdefinition** können Sie eigene Filter definieren und auf die jeweilige Spalte anwenden.

25.1.2 Bestandinformationen aktualisieren

Die Benutzer-PCs übertragen die jeweils aktuellen Bestandinformationen, wenn sich die Informationen geändert haben.

Über den Befehl **Aktualisierung anfordern** können Sie manuell eine Aktualisierung der Bestandinformationen anfordern. Dieser Befehl steht für einen einzelnen oder alle Computer eines Knotens über das Kontextmenü sowie über das Menü **Aktionen** in der SafeGuard Management Center Menüleiste zur Verfügung. Darüber hinaus lässt sich der Befehl über das Kontextmenü der Listeneinträge auswählen.

Wenn Sie diesen Befehl auswählen oder auf das Symbol **Aktualisierung anfordern** in der Symbolleiste klicken, übertragen die jeweiligen Benutzer-PCs ihre aktuellen Bestandinformationen. Wählen Sie den Befehl für einen Knoten, so werden alle Computer im Knoten sowie in allen Unterknoten einbezogen.

Für die Aktualisierung der Ansicht im SafeGuard Management Center steht wie für andere Bereiche des Management Centers der Befehl **Aktualisieren** im Kontextmenü für den einzelnen oder alle Computer eines Knotens sowie im Menü **Ansicht** in der Menüleiste zur Verfügung. Zur Aktualisierung der Ansicht können Sie auch das Doppelpfeilsymbol **Aktualisieren** in der Symbolleiste wählen.

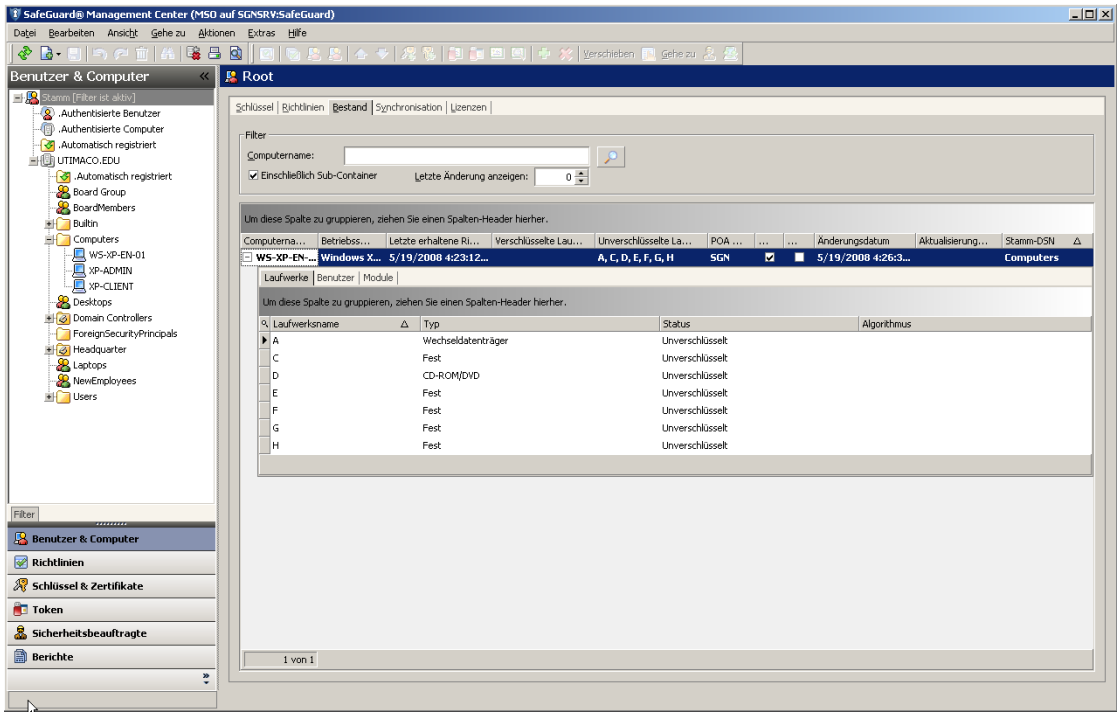
25.1.3 Übersicht

Die einzelnen Spalten der Übersicht zeigen folgende Informationen:

Spalte	Erklärung
Computername	Zeigt den Namen des Computers.
Betriebssystem	Zeigt das Betriebssystem des Computers.
Letzte erhaltene Richtlinie	Zeigt an, wann (Datum und Uhrzeit) der Client die letzte Richtlinie erhalten hat.
Verschlüsselte Laufwerke	Zeigt die verschlüsselten Laufwerke des Computers.
Unverschlüsselte Laufwerke	Zeigt die unverschlüsselten Laufwerke des Computers.
POA Typ	Gibt an, ob es sich bei dem betreffenden Computer um einen BitLocker Client oder einen nativen SafeGuard Enterprise Client handelt.
POA	Gibt an, ob die Power-on Authentication für den Computer aktiviert ist.
WOL	Gibt an, ob Wake On LAN für den Computer aktiviert ist.
Änderungsdatum	Zeigt das Datum, an dem sich die Bestandsinformationen durch Anforderung einer Bestandsaktualisierung oder Übermittlung neuer Bestandsinformationen vom Client geändert haben.
Aktualisierung angefordert	Zeigt das Datum der letzten Aktualisierungsanforderung an. Der in diesem Feld angezeigte Wert wird bei der Verarbeitung der Anforderung durch den Client wieder gelöscht.
Stamm-DSN	Zeigt den Distinguished Name des dem Computer übergeordneten Containerobjekts an. Diese Spalte wird nur dann angezeigt, wenn im **Filter**-Bereich das Feld **Einschließlich Sub-Container** aktiviert wurde.

25.1.4 Registerkarte Laufwerke

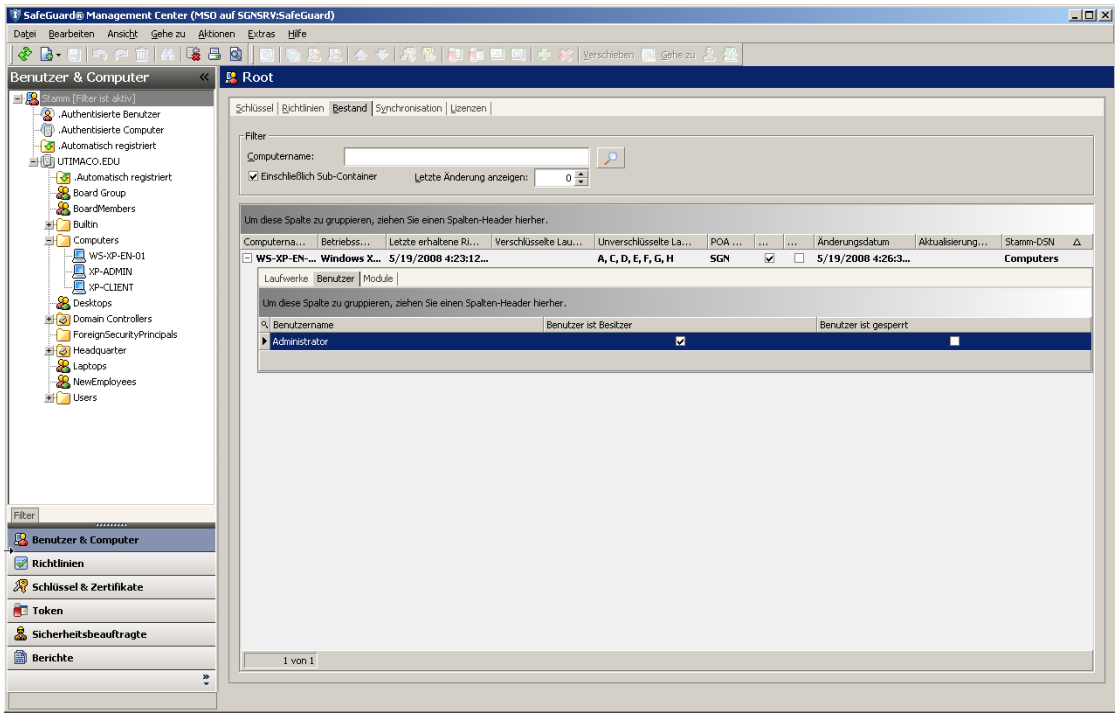
Die Registerkarte **Laufwerke** zeigt Bestand- und Statusinformationen zu den Laufwerken des jeweiligen Computers.



Spalte	Erklärung
Laufwerksname	Zeigt den Laufwerksnamen an.
Typ	Zeigt den Laufwerkstyp an, z. B. Fest, Wechseldatenträger oder CD-ROM/DVD.
Status	Zeigt den Verschlüsselungsstatus des Laufwerks an.
Algorithmus	Zeigt für verschlüsselte Laufwerke den Algorithmus, der zur Verschlüsselung benutzt wurde, an.

25.1.5 Registerkarte Benutzer

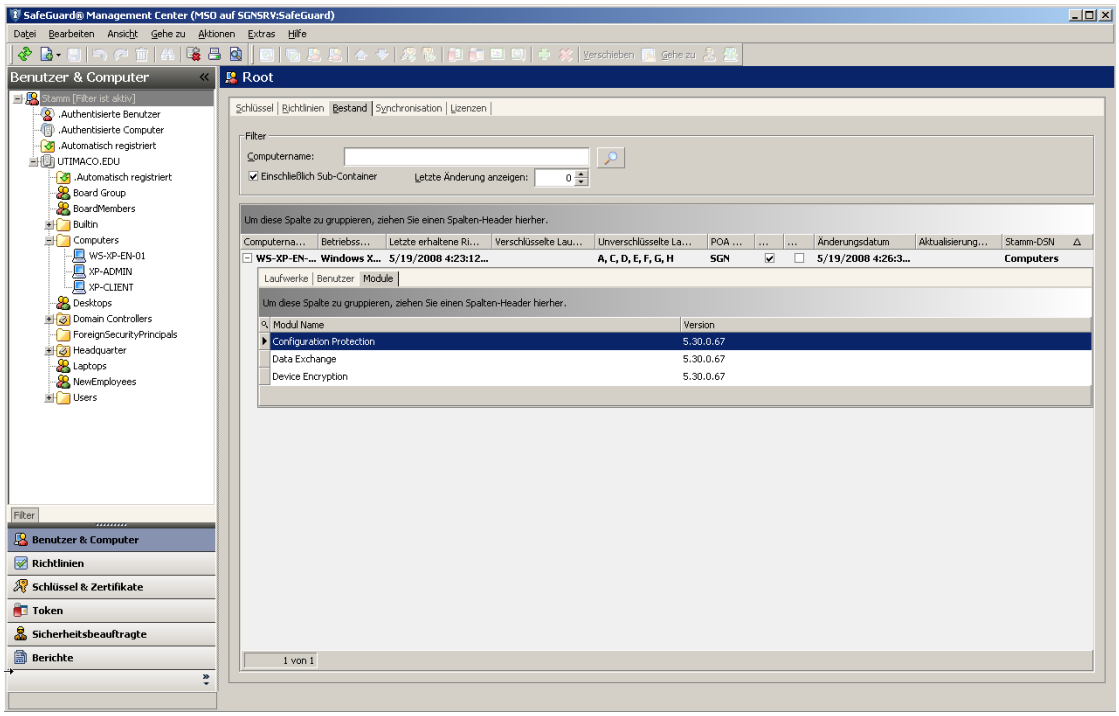
Die Registerkarte **Benutzer** zeigt Bestand- und Statusinformationen zu den Benutzern des jeweiligen Computers.


SafeGuard® Management Center (MSO auf SGNSRV:SafeGuard)
Datei Bearbeiten Ansicht Gehe zu Aktionen Extras Hilfe
Benutzer & Computer
Root
Schlüssel Richtlinien Bestand Synchronisation Lizenzen
Filter
Computername:
Einschließlich Sub-Container
Letzte Änderung anzeigen:
Um diese Spalte zu gruppieren, ziehen Sie einen Spalten-Header hierher.
Computerna... Betriebss... Letzte erhaltene Ri... Verschlüsselte Lau... Unverschlüsselte La... POA ... Änderungsdatum Aktualisierung... Stamm-DSN
WS-XP-EN-... Windows X... 5/19/2008 4:23:12... A, C, D, E, F, G, H SGN 5/19/2008 4:26:3... Computers
Laufwerke Benutzer Module
Um diese Spalte zu gruppieren, ziehen Sie einen Spalten-Header hierher.
Benutzername Benutzer ist Besitzer Benutzer ist gesperrt
Administrator
1 von 1
Benutzer & Computer
Richtlinien
Schlüssel & Zertifikate
Token
Sicherheitsbeauftragte
Berichte

Spalte	Erklärung
Benutzername	Zeigt den Benutzernamen des jeweiligen Benutzers.
Benutzer ist Besitzer	Gibt an, ob der Benutzer als Besitzer der Maschine definiert ist.
Benutzer ist gesperrt	Gibt an, ob der Benutzer gesperrt ist.

25.1.6 Registerkarte Module

Die Registerkarte **Module** liefert eine Übersicht zu allen auf dem Computer installierten SafeGuard Enterprise Modulen.


SafeGuard® Management Center (MSO auf SGNSRV:SafeGuard)
Datei Bearbeiten Ansicht Gehe zu Aktionen Extras Hilfe
Benutzer & Computer
Root
Schlüssel Richtlinien Bestand Synchronisation Lizenzen
Filter
Computername:
Einschließlich Sub-Container
Letzte Änderung anzeigen:
Um diese Spalte zu gruppieren, ziehen Sie einen Spalten-Header hierher.
Computerna... Betriebss... Letzte erhaltene Ri... Verschlüsselte Lau... Unverschlüsselte La... POA ... Änderungsdatum Aktualisierung... Stamm-DSN
WS-XP-EN-... Windows X... 5/19/2008 4:23:12... A, C, D, E, F, G, H SGN 5/19/2008 4:26:3... Computers
Laufwerke Benutzer Module
Um diese Spalte zu gruppieren, ziehen Sie einen Spalten-Header hierher.
Modul Name
Version
Configuration Protection 5.30.0.67
Data Exchange 5.30.0.67
Device Encryption 5.30.0.67
1 von 1
Benutzer & Computer
Richtlinien
Schlüssel & Zertifikate
Token
Sicherheitsbeauftragte
Berichte

Spalte	Erklärung
Module Name	Zeigt den Namen des installierten SafeGuard Enterprise Moduls.
Version	Zeigt die Software-Version des installierten SafeGuard Enterprise Moduls.

25.2 Bestandberichte drucken

Die in der Registerkarte **Bestand** angezeigten Informationen lassen sich über das **Datei**-Menü in der Menüleiste des SafeGuard Management Centers als Bestandberichte drucken.

Um vor dem Drucken eine Druckvorschau zu erstellen, wählen Sie **Datei** > **Druckvorschau**. In der Druckvorschau stehen verschiedene Funktionen, zum Beispiel für den Export des Dokuments in eine Reihe von Ausgabeformaten (zum Beispiel .PDF) oder die Bearbeitung des Seitenlayouts (zum Beispiel Kopf- und Fußzeile), zur Verfügung.

Um das Dokument sofort zu drucken, wählen Sie **Datei** > **Drucken**.

26 Berichte

Die Aufzeichnung sicherheitsrelevanter Vorfälle ist Voraussetzung für eine gründliche Systemanalyse. Anhand der protokollierten Ereignisse können Vorgänge auf einer Arbeitsstation bzw. innerhalb eines Netzwerks exakter nachvollzogen werden. Durch die Protokollierung lassen sich zum Beispiel Schutzverletzungen unautorisierter Dritter nachweisen. Dem Administrator bzw. Sicherheitsbeauftragten bietet die Protokollierung auch eine Hilfe, um irrtümlich verwehrte Benutzerrechte ausfindig zu machen und zu korrigieren.

SafeGuard Enterprise protokolliert alle Client-Aktivitäten und -Statusinformationen sowie Administratoraktionen und sicherheitsrelevante Ereignisse und speichert diese zentral. Die Protokollierung zeichnet Ereignisse auf, die installierte SafeGuard Produkte auslösen. Die Art der Protokolle wird in Protokollierungsrichtlinien festgelegt. Hier wird auch der Ausgabe- und Speicherort der protokollierten Ereignisse definiert: die Windows-Ereignisanzeige des jeweiligen Clients oder die SafeGuard Enterprise Datenbank.

Als Sicherheitsbeauftragter mit den entsprechenden Rechten können Sie die im SafeGuard Management Center angezeigten Statusinformationen und Protokollberichte einsehen, ausdrucken und archivieren. Umfassende Sortier- und Filterfunktionen unterstützen Sie bei der Auswahl relevanter Ereignisse aus den verfügbaren Informationen.

Auch eine automatisierte Auswertung der Log-Datenbank, zum Beispiel über Crystal Reports oder Microsoft System Center Operations Manager, ist möglich. Die Protokolleinträge werden von SafeGuard Enterprise sowohl auf Client- als auch auf Server-Seite durch Signatur gegen unbefugte Manipulation geschützt.

Gemäß der definierten und zugewiesenen Protokollierungsrichtlinie können Ereignisse aus den folgenden Kategorien protokolliert werden:

- Anmeldung
- Administration
- System
- Verschlüsselung
- Client
- Kommunikation
- Zugriffskontrolle

26.1 Anwendungsgebiete

Die SafeGuard Enterprise Protokollierung von Ereignissen ist eine benutzerfreundliche und umfassende Lösung zum Aufzeichnen und Auswerten von Ereignissen. Die folgenden Beispiele zeigen einige typische Anwendungsszenarien für die SafeGuard Enterprise **Berichte**-Funktionalität.

Zentrale Überwachung von Arbeitsstationen im Netzwerk

Der zuständige Sicherheitsbeauftragte will regelmäßig über kritische Ereignisse (zum Beispiel Zugriff auf Dateien, für die ein Benutzer keine Berechtigung hat, oder eine Reihe von fehlgeschlagenen Anmeldungsversuchen innerhalb eines bestimmten Zeitraums) informiert werden. Über eine Protokollierungsrichtlinie lässt sich die Protokollierung so konfigurieren, dass alle auf den relevanten Benutzer-PCs auftretenden sicherheitskritischen Ereignisse in einer lokalen Protokolldatei protokolliert und beim Erreichen einer ebenfalls in einer Richtlinie festgelegten Anzahl an Ereignissen über den SafeGuard Enterprise Server in die SafeGuard Enterprise Datenbank übertragen werden. In der Ereignisanzeige des SafeGuard Management Centers kann der Sicherheitsbeauftragte die Ereignisse abrufen, einsehen und analysieren. Somit lassen sich die Vorgänge auf den verschiedenen Benutzer-PCs kontrollieren, ohne dass Mitarbeiter Einfluss auf die Aufzeichnungen nehmen können.

Überwachen mobiler Benutzer

Mobile Benutzer sind in der Regel nicht ständig mit dem Unternehmensnetzwerk verbunden. Ein Außendienstmitarbeiter nimmt zum Beispiel für einen Termin sein Notebook vom Netz. Sobald er sich wieder am Netzwerk anmeldet, werden die während der Offline-Zeit protokollierten SafeGuard Enterprise Ereignisse übertragen. Die Protokollierung liefert somit einen genauen Überblick über die Benutzeraktivitäten während der betreffende Computer nicht an das Netzwerk angeschlossen war.

26.2 Voraussetzung

Eine Maschine, auf der nur das SafeGuard Management Center installiert ist, hat nach der ersten Installation keine Verbindung zum Server. Für die Nutzung der Protokollierung ist es in diesem Fall notwendig, auf dieser Maschine das Client-Paket auszuführen. Dadurch wird die Maschine beim Server als Client aktiviert und die Protokollierungsfunktionalität kann benutzt werden.

Weitere Informationen zum Client-Paket finden Sie im SafeGuard Enterprise Installationshandbuch.

26.3 Ziel für protokollierte Ereignisse

Ziel der protokollierten Ereignisse kann die Windows-Ereignisanzeige oder die SafeGuard Enterprise Datenbank sein. In das jeweilige Ziel schreibt die Protokollierung nur Ereignisse, die mit einem SafeGuard-Produkt verknüpft sind. Die Ausgabeziele für zu protokollierende Ereignisse werden in der Protokollierungsrichtlinie festgelegt.

26.3.1 Windows-Ereignisanzeige

Ereignisse, für die Sie in der Protokollierungsrichtlinie die Windows-Ereignisanzeige als Ziel festlegen, werden in der Windows-Ereignisanzeige abgelegt. Über die Windows-Ereignisanzeige lassen sich Protokolle für System-, Sicherheits- und Anwendungs-Ereignisse anzeigen und verwalten sowie die Ereignisprotokolle sichern. Für diese Vorgänge benötigen Sie einen Administrator-Account für den jeweiligen Client. In der Ereignisanzeige wird jeweils ein Fehlercode, kein beschreibender Text des Ereignisses, angezeigt.

Hinweis: Dieses Kapitel beschreibt das Einsehen sowie die Verwaltung und Analyse der Ereignisprotokolle im SafeGuard Management Center. Weitere Informationen zum Einsehen und Verwalten von Ereignisprotokollen über die Windows-Ereignisanzeige finden Sie in Ihrer Microsoft-Dokumentation.

26.3.2 SafeGuard Enterprise Datenbank

Ereignisse, für die Sie in der Protokollierungsrichtlinie die SafeGuard Enterprise Datenbank als Ziel festlegen, werden in lokalen Protokolldateien im Local Cache des jeweiligen Benutzer-PCs im Verzeichnis auditing\SGMTranslog gesammelt. Diese Dateien werden an den Transportmechanismus übergeben, der sie dann über den SafeGuard Enterprise Server in die Datenbank einträgt. Die Übergabe erfolgt standardmäßig immer dann, wenn der Transportmechanismus erfolgreich eine Verbindung zum Server aufbauen konnte. Um die Größe einer Protokolldatei einzuschränken, können Sie in einer Richtlinie des Typs **Allgemeine Einstellungen** eine maximale Anzahl an Protokolleinträgen definieren. Die Protokolldatei wird dann vom Protokollsystem nach Erreichen der festgelegten Anzahl an Einträgen in die Transportqueue des SafeGuard Enterprise Servers gestellt. Danach wird eine neue Protokolldatei begonnen. Die in der zentralen Datenbank protokollierten Ereignisse lassen sich in der SafeGuard Enterprise Ereignisanzeige abrufen. Für das Einsehen, Analysieren und Verwalten der in der Datenbank protokollierten Ereignisse benötigen Sie als Sicherheitsbeauftragter die relevanten Berechtigungen.

26.4 Einstellungen für die Protokollierung festlegen

Die Definition von Berichten erfolgt über zwei Richtlinien:

- Richtlinie des Typs **Allgemeine Einstellungen**
  In einer Richtlinie des Typs **Allgemeine Einstellungen** können Sie die Anzahl an protokollierten Ereignissen angeben, nach deren Erreichen die Protokolldatei mit den für die zentrale Datenbank bestimmten Ereignissen an die SafeGuard Enterprise Datenbank übermittelt werden soll. Dadurch wird die Größe der einzelnen zu übertragenden Protokolldateien begrenzt. Diese Einstellung ist optional.
- Richtlinie des Typs **Protokollierung**
  Die zu protokollierenden Ereignisse werden in der Protokollierungsrichtlinie definiert. Hier legen Sie als Sicherheitsbeauftragter mit den relevanten Berechtigungen fest, welche Ereignisse an welchem Ausgabeort protokolliert werden.

Die folgenden beiden Abschnitte beschreiben die Definition dieser beiden Richtlinien für die Protokollierung.

26.4.1 Anzahl an Ereignissen für Rückmeldung festlegen

So definieren Sie in einer Richtlinie die Anzahl an Ereignissen, nach deren Erreichen die Protokolldatei übermittelt werden soll:

1. Sie befinden sich im geöffneten Management Center im Bereich **Richtlinien**.
2. Legen Sie eine neue Richtlinie des Typs **Allgemeine Einstellung** an oder wählen Sie eine bereits bestehende Richtlinie aus.
3. Legen Sie im Feld **Rückmeldung nach Anzahl von Ereignissen** die Anzahl an Ereignissen fest, nach deren Erreichen die Protokolldatei mit den für die zentrale Datenbank bestimmten Einträgen übertragen werden soll.
4. Speichern Sie Ihre Einstellungen.

Nach der Zuweisung der Richtlinie gilt die festgelegte Anzahl von Ereignissen für die Protokollierung.

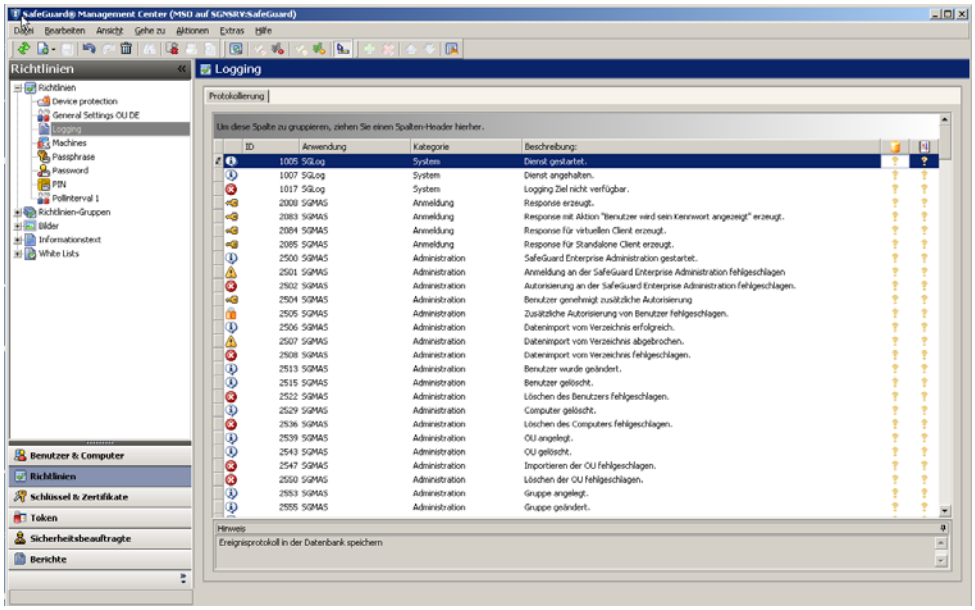
26.4.2 Ereignisse für die Protokollierung auswählen

So wählen Sie die Ereignisse für die Protokollierung aus:

Sie befinden sich im geöffneten Management Center im Bereich **Richtlinien**.

1. Legen Sie eine neue Richtlinie des Typs **Protokollierung** an oder wählen Sie eine bereits bestehende Richtlinie aus.

2. Im rechten Aktionsbereich unter **Protokollierung** werden die vordefinierten Ereignisse, die protokolliert werden können, angezeigt. Ein Klick auf die Spaltenüberschrift sortiert die Ereignisse nach **ID**, **Kategorie** usw.



3. Um festzulegen, dass ein Ereignis in der SafeGuard Enterprise Datenbank protokolliert werden soll, wählen Sie das Ereignis in der Spalte mit dem Datenbanksymbol **Ereignisse in der Datenbank protokollieren** durch Klicken mit der Maus aus. Für Ereignisse, die in der Windows-Ereignisanzeige protokolliert werden sollen, klicken Sie in der Spalte mit dem Ereignisprotokollsymbol **Im Ereignisprotokoll protokollieren**. Durch wiederholtes Klicken lässt sich die Markierung wieder aufheben oder auf null setzen.

   Für Ereignisse, für die Sie keine Einstellung festlegen, gelten die vordefinierten Standardwerte. Um die geltenden Standardwerte einzublenden, klicken Sie auf das Standardwerte-Lupensymbol **Standardwerte für nicht konfigurierte Einstellungen anzeigen** in der SafeGuard Management Center Symbolleiste.

Hinweis: Sie können diese Einstellungen auch über das Kontextmenü bei den einzelnen Ereignissen definieren.

4. Bei den für die Protokollierung ausgewählten Ereignissen wird in der betreffenden Spalte ein grünes Häkchen angezeigt.
   Speichern Sie Ihre Einstellungen.

Nach der Zuweisung der Richtlinie werden die ausgewählten Ereignisse am festgelegten Ausgabeziel protokolliert.

Auswählbare Ereignisse

Für eine Auflistung aller für die Protokollierung auswählbaren Ereignisse, siehe *Für Berichte auswählbare Ereignisse* auf Seite 310.

26.5 Protokollierte Ereignisse einsehen

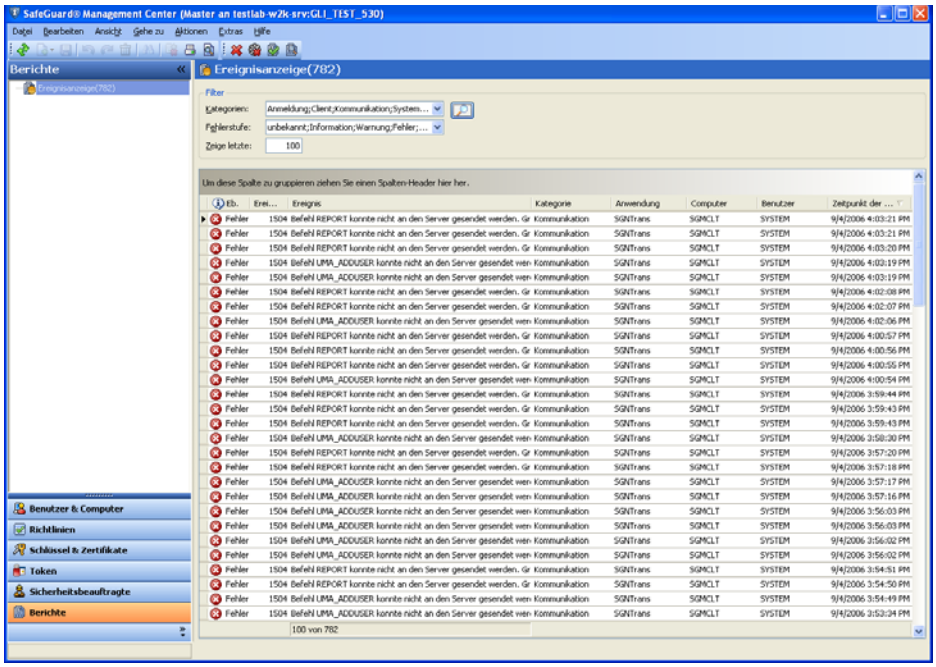
Wenn Sie als Sicherheitsbeauftragter über die entsprechenden Berechtigungen verfügen, können Sie die in der zentralen Datenbank protokollierten Ereignisse in der SafeGuard Management Center Ereignisanzeige einsehen.

So rufen Sie in der zentralen Datenbank protokollierte Ereignisse ab:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Centers auf die Schaltfläche **Berichte**.

2. Klicken Sie im rechten Fensterbereich **Ereignisanzeige** auf das Lupensymbol.

Alle in der zentralen Datenbank protokollierten Ereignisse werden in der Ereignisanzeige angezeigt.



Die einzelnen Spalten zeigen folgende Informationen zu den protokollierten Ereignissen:

Spalte	Erklärung
Ebene (Symbol)	Zeigt ein Symbol, das die Klassifizierung des Ereignisses, z. B. Warnung, Fehler, angibt.
Ereignis-ID	Zeigt eine Nummer zur Identifizierung des Ereignisses.
Ereignis	Zeigt den Ereignistext, d.h. eine Beschreibung des Ereignisses.
Kategorie	Zeigt die Klassifizierung des Ereignisses durch die Quelle, z. B.: Verschlüsselung, Anmeldung, System.
Anwendung	Zeigt den Bereich der Software, der das Ereignis übermittelt hat, z. B. SGMAuth, SGBaseENc, SGMAS.
Computer	Zeigt den Namen des Computers, auf dem das protokollierte Ereignis aufgetreten ist.
Computerdomäne	Zeigt die Domäne des Computers, auf dem das protokollierte Ereignis aufgetreten ist.
Benutzer	Zeigt den Benutzer, der beim Auftreten des Ereignisses angemeldet war.
Benutzerdomäne	Zeigt die Domäne des Benutzers, der beim Auftreten des Ereignisses angemeldet war.
Zeitpunkt der Protokollierung	Zeigt Systemdatum und Systemuhrzeit der Protokollierung des Ereignisses auf dem Client.

Durch Klicken auf den Spalten-Header lässt sich die Ereignisanzeige nach **Ebene**, **Kategorie** usw. sortieren.

Darüber hinaus steht über das Kontextmenü der einzelnen Spalten eine Reihe von Funktionen für die Sortierung, Gruppierung und Anpassung der Ereignisanzeige zur Verfügung.

Wenn Sie auf einen Eintrag in der Ereignisanzeige doppelklicken, werden Details zum protokollierten Ereignis angezeigt.

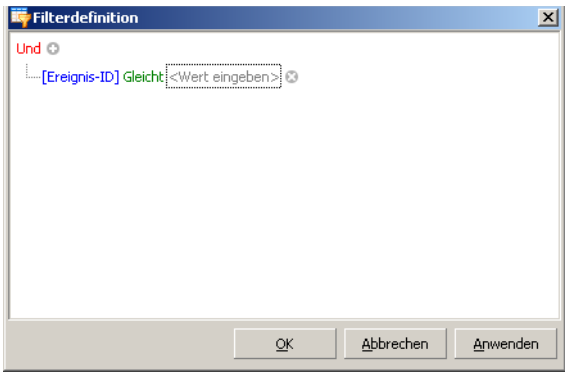
26.5.1 SafeGuard Enterprise Ereignisanzeige filtern

Das SafeGuard Management Center bietet umfassende Filterfunktionen, mit deren Hilfe Sie die jeweils relevanten Ereignisse schnell aus Fülle der in der Ereignisanzeige dargestellten Informationen ermitteln können.

Im **Filter**-Bereich der **Ereignisanzeige** stehen folgende Felder für die Definition von Filtern zur Verfügung:

Feld	Beschreibung
Kategorien	Unter Anwendung dieses Felds lässt sich die Ereignisanzeige nach den in der Spalte **Kategorie** angegebenen Klassifizierungen durch die Quelle (zum Beispiel Verschlüsselung, Anmeldung, System) filtern. Wählen Sie hierzu die gewünschten Kategorien in der Dropdownliste des Felds aus.
Fehlerstufe	Unter Anwendung dieses Felds lässt sich die Ereignisanzeige nach den in der Spalte **Ebene** angegebenen Windows-Ereignisklassifizierungen (z. B. Warnung, Fehler) filtern. Wählen Sie hierzu die gewünschten Ebenen in der Dropdownliste des Felds aus.
Zeige letzte	In diesem Feld können Sie die Anzahl der anzuzeigenden Ereignisse festlegen. Es werden jeweils die zuletzt protokollierten Ereignisse (standardmäßig die 100 letzten Ereignisse) angezeigt.

Darüber hinaus können Sie mit dem Filter-Editor benutzerdefinierte Filter erstellen. Der Filter-Editor lässt sich über das Kontextmenü der einzelnen Berichtsspalten aufrufen. Im Fenster **Filterdefinition** können Sie eigene Filter definieren und auf die jeweilige Spalte anwenden.



26.6 Berichte drucken

Die in der SafeGuard Management Center Ereignisanzeige angezeigten Ereignisberichte lassen sich über das **Datei**-Menü in der Menüleiste des SafeGuard Management Centers drucken.

Um vor dem Drucken eine Druckvorschau zu erstellen, wählen Sie **Datei** > **Druckvorschau**. In der Druckvorschau stehen verschiedene Funktionen, zum Beispiel für den Export des Dokuments in eine Reihe von Ausgabeformaten (zum Beispiel .PDF) oder die Bearbeitung des Seitenlayouts (zum Beispiel Kopf- und Fußzeile), zur Verfügung.

Um das Dokument sofort zu drucken, wählen Sie **Datei** > **Drucken**.

26.7 Verkettung von protokollierten Ereignissen

Die für die zentrale Datenbank bestimmten Ereignisse werden in der EVENT-Tabelle der SafeGuard Enterprise Datenbank protokolliert. Auf diese Tabelle kann ein spezieller Integritätsschutz angewendet werden. Die Ereignisse lassen sich als verkettete Liste in der EVENT-Tabelle protokollieren. Durch die Verkettung ist ein Eintrag in der Liste jeweils von seinem Vorgängereintrag abhängig. Wird ein Eintrag aus der Liste entfernt, so ist dies sichtbar und über eine Integritätsprüfung nachweisbar.

Zur Optimierung der Performance ist die Verkettung der Ereignisse in der EVENT-Tabelle standardmäßig deaktiviert. Zur Überprüfung der Integrität der protokollierten Ereignsse (siehe *Integrität protokollierter Ereignisse prüfen* auf Seite 296) können Sie jedoch die Verkettung auch aktivieren.

Achtung: Wenn die Verkettung von protokollierten Ereignissen deaktiviert ist, gilt kein spezieller Integritätsschutz für die EVENT-Tabelle.

26.7.1 Verkettung protokollierter Ereignisse aktivieren

So aktivieren Sie die Verkettung protokollierter Ereignisse:

1. Stoppen Sie den Webservice SGNSRV auf dem Web Server.
2. Löschen Sie alle Ereignisse aus der Datenbank und erstellen Sie während des Löschvorgangs eine Sicherungskopie, siehe *Ausgewählte oder alle Ereignisse löschen* auf Seite 296.

Hinweis: Wenn Sie die alten Ereignisse nicht aus der Datenbank löschen, funktioniert die Verkettung nicht, da für die verbleibenden alten Ereignisse die Verkettung nicht aktiviert war.

3. Setzen Sie folgenden Registry Key auf 0 oder löschen Sie ihn:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Utimaco\SafeGuard Enterprise
DWORD: DisableLogEventChaining = 0
```

4. Starten Sie den Webservice neu.

Die Verkettung ist wieder aktiviert.

Um die Verkettung wieder zu deaktivieren, setzen Sie den Registry Key auf `1`.

26.8 Integrität protokollierter Ereignisse prüfen

Voraussetzung: Für die Überprüfung der Integrität von protokollierten Ereignissen muss die Verkettung der Ereignisse in der EVENT-Tabelle aktiviert sein.

So prüfen Sie die Integrität der in der SafeGuard Enterprise **Ereignisanzeige** angezeigten Ereignisse:

Sie befinden sich im geöffneten Management Center im Bereich **Berichte**.

Wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen** > **Integrität prüfen** oder klicken Sie in der Symbolleiste auf das Symbol **Integrität von protokollierten Ereignissen prüfen**.

Eine Meldung liefert die Informationen zur Integrität der protokollierten Ereignisse.

Hinweis: Wenn die Verkettung der Ereignisse deaktiviert ist, wird bei der Überprüfung der Integrität protokollierter Ereignisse im SafeGuard Management Center ein Fehler ausgegeben.

26.9 Ausgewählte oder alle Ereignisse löschen

So löschen Sie ausgewählte Ereignisse aus dem Ereignisprotokoll:

Sie befinden sich im geöffneten Management Center im Bereich **Berichte**.

1. Markieren Sie in der **Ereignisanzeige** die Ereignisse, die gelöscht werden sollen.
2. Um ausgewählte Ereignisse zu löschen, wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen** > **Ereignisse löschen** oder klicken Sie in der Symbolleiste auf das Symbol **Ausgewählte Ereignisse löschen**.
   Um alle Ereignisse zu löschen, wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen** > **Alle Ereignisse löschen** oder klicken Sie in der Symbolleiste auf das Symbol **Alle Ereignisse löschen**.
3. Vor dem Löschen der ausgewählten Ereignisse wird ein Fenster zur Erstellung einer Sicherungsdatei angezeigt, siehe *Sicherungsdatei erstellen* auf Seite 297.

Die ausgewählten Ereignisse sind aus dem Ereignisprotokoll gelöscht.

26.10 Sicherungsdatei erstellen

Sicherungsdateien von den in der Ereignisanzeige angezeigten Berichten lassen sich im Rahmen des Löschvorgangs erstellen.

Wenn Sie **Aktionen** > **Ereignisse löschen** oder **Aktionen** > **Alle Ereignisse löschen** wählen, wird vor dem Löschen der Ereignisse das Fenster **Ereignisse sichern als** zur Erstellung einer Sicherungsdatei angezeigt. Um eine Sicherung des Ereignisprotokolls in Form einer XML-Datei zu erstellen, geben Sie einen Dateinamen und einen Speicherort an und klicken Sie auf **OK**.

26.11 Sicherungsdatei öffnen

So öffnen Sie die im Rahmen eines Löschvorgangs erstellte XML-Sicherungsdatei.

Sie befinden sich im geöffneten Management Center unter **Berichte**.

1. Wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen** > **Sicherungsdatei öffnen** oder klicken Sie in der Symbolleiste auf das Symbol **Sicherungsdatei öffnen**.
2. Das Fenster **Sicherung öffnen** wird angezeigt. Wählen Sie die zu öffnende Sicherungsdatei aus und klicken Sie auf **Öffnen**.

Die Sicherungsdatei wird geöffnet und die Ereignisse werden in der Ereignisanzeige angezeigt. Um wieder zur regulären Ansicht der Ereignisanzeige zurückzukehren, klicken Sie erneut auf das Symbol **Sicherungsdatei öffnen** in der Symbolleiste.

26.12 Regelmäßige Säuberung der EVENT-Tabelle über Skript

Für die automatische und effiziente Säuberung der EVENT-Tabelle stehen im \tools Verzeichnis Ihrer SafeGuard Enterprise Produkt-CD vier SQL Skripte zur Verfügung:

- `spShrinkEventTable_install.sql`
- `ScheduledShrinkEventTable_install.sql`
- `spShrinkEventTable_uninstall.sql`
- `ScheduledShrinkEventTable_uninstall.sql`

Die beiden Skripte `spShrinkEventTable_install.sql` und `ScheduledShrinkEventTable_install.sql` installieren eine gespeicherte Prozedur am Datenbankserver sowie einen Scheduled Job, der die gespeicherte Prozedur in definierten regelmäßigen Abständen ausführen lässt. Die gespeicherte Prozedur verschiebt Ereignisse aus der EVENT-Tabelle in die Backup-Log-Tabelle EVENT_BACKUP. Dabei wird eine definierte Anzahl an neuesten Ereignissen in der EVENT-Tabelle belassen.

Die beiden Skripte `spShrinkEventTable_uninstall.sql` und `ScheduledShrinkEventTable_uninstall.sql` deinstallieren die gespeicherte Prozedur sowie den Scheduled Job und löschen die Tabelle EVENT_BACKUP.

Achtung: Wenn Sie die Ereignisse über die gespeicherte Prozedur aus der EVENT-Tabelle in die Backup-Log-Tabelle verschieben, findet die Verkettung der Protokollierung keine Anwendung mehr. Es ist daher nicht sinnvoll, die Verkettung zu aktivieren und gleichzeitig die gespeicherte Prozedur zur Säuberung der EVENT-Tabelle einzusetzen. Für weitere Informationen zur Verkettung von Ereignissen siehe *Verkettung von protokollierten Ereignissen* auf Seite 295.

26.12.1 Gespeicherte Prozedur erstellen

Das Skript `spShrinkEventTable_install.sql` erstellt eine gespeicherte Prozedur, die Daten aus der EVENT-Tabelle in eine Backup-Log-Tabelle mit dem Namen EVENT_BACKUP verschiebt. Wenn die Tabelle EVENT_BACKUP noch nicht vorhanden ist, wird sie automatisch erstellt.

Die erste Zeile lautet „USE SafeGuard“. Wenn Sie für Ihre SafeGuard Enterprise Datenbank einen anderen Namen als „SafeGuard“ verwendet haben, ändern Sie den Namen hier entsprechend.

Die gespeicherte Prozedur belässt die <n> neuesten Ereignisse in der EVENT-Tabelle und verschiebt den Rest in die Tabelle EVENT_BACKUP. Die Anzahl an Ereignissen, die in der EVENT-Tabelle verbleiben sollen, wird über einen Parameter festgelegt.

Um die gespeicherte Prozedur auszuführen, verwenden Sie folgenden Befehl in SQL Server Management Studio (New Query):

```
exec spShrinkEventTable 1000
```

Bei Verwendung dieses Beispielbefehls werden alle Ereignisse außer den neuesten 1000 verschoben.

26.12.2 Scheduled Job für die Ausführung der gespeicherten Prozedur anlegen

Um die EVENT-Tabelle in regelmäßigen Abständen automatisch zu säubern, können Sie einen Job am SQL Server anlegen.
Dieser Job kann über das Skript `ScheduledShrinkEventTable_install.sql` oder über den SQL Enterprise Manager erstellt werden.

Achtung: Der Job funktioniert nicht bei SQL Express Datenbanken. Damit der Job ausgeführt werden kann, muss der SQL Server Agent laufen. Da bei SQL Server Express Installation kein SQL Server Agent vorhanden ist, werden Jobs hier nicht unterstützt.

- Der Skript-Teil muss in der msdb ausgeführt werden. Wenn Sie für Ihre SafeGuard Enterprise Datenbank einen anderen Namen als SafeGuard ausgewählt haben, ändern Sie den Namen entsprechend.

  ```
  /* Default: Database name 'SafeGuard' change if required*/
  SELECT @SafeGuardDataBase='SafeGuard'
  ```

- Sie können auch die Anzahl an Ereignissen festlegen, die in der EVENT-Tabelle verbleiben sollen. Die Standardeinstellung ist 100.000.

  ```
  /* Default: keep the latest 100000 events, change if required*/
  SELECT @ShrinkCommand='exec spShrinkEventTable 100000'
  ```

- Sie können festlegen, ob die Ausführung des Jobs im NT Event Log protokolliert werden soll.

  ```
  exec sp_add_job
  @job_name='AutoShrinkEventTable',
  @enabled=1,
  @notify_level_eventlog=3
  ```

  Für den Parameter `notify_level_eventlog` sind folgende Werte verfügbar:

Wert	Ergebnis
3	Jede Ausführung des Jobs protokollieren.
2	Fehlschlagen des Jobs protokollieren.
1	Erfolgreiche Ausführung des Jobs protokollieren.
0	Ausführung des Jobs nicht im NT Event Log protokollieren.

- Sie können festlegen, wie oft die Ausführung des Jobs im Fall eines Fehlschlags wiederholt werden soll.

  ```
  exec sp_add_jobstep
  ```

  - `@retry_attempts=3`
    Dieses Beispiel legt 3 Versuche für die Ausführung des Jobs im Fall eines Fehlschlags fest.
  - `@retry_interval=60`
    Dieses Beispiel legt fest, dass die Ausführung des Jobs in einem Abstand von 60 Minuten wiederholt werden soll.

- Sie können einen Zeitplan für die Ausführung des Jobs festlegen.

  ```
  exec sp_add_jobschedule
  ```

  - `@freq_type=4`
    Dieses Beispiel legt fest, dass der Job täglich ausgeführt wird.

- `@freq_interval=1`
  Dieses Beispiel legt fest, dass der Job einmal pro Tag ausgeführt wird.
- `@active_start_time=010000`
  Dieses Beispiel legt fest, dass der Job um 01:00 Uhr ausgeführt wird.

Achtung: Die für Parameter `@active_start_time` oben angegebene Syntax funktioniert mit SQL Server 2005. Die korrekte Syntax für SQL Server 2000 lautet: `@active_start_time='1:00:00'.`

Hinweis: Neben den oben angeführten Beispielwerten lässt sich noch eine Vielzahl von verschiedenen Zeitplanoptionen mit `sp_add-jobschedule` definieren. So lässt sich der Job zum Beispiel alle zwei Minuten oder nur einmal pro Woche ausführen. Detaillierte Informationen hierzu finden Sie in der Microsoft Transact SQL Dokumentation.

26.12.3Gespeicherte Prozeduren, Jobs und Tabellen löschen

Das Skript `spShrinkEventTable` löscht die gespeicherte Prozedur sowie die EVENT-BACKUP Tabelle. Das Skript `ScheduledShrinkEventTable_uninstall.sql` deaktiviert den Scheduled Job.

Achtung: Wenn Sie `spShrinkEventTable` ausführen, wird die Tabelle EVENT_BACKUP mit allen enthaltenen Daten vollständig gelöscht.

26.13 Texte für Ereignisberichte

In der SafeGuard Enterprise Datenbank werden die Ereignisse nicht mit kompletten Ereignistexten protokolliert sondern jeweils nur mit ihrer ID sowie mit den entsprechenden Parameterwerten in die Datenbanktabelle geschrieben. Beim Abrufen der Ereignisse werden die Parameterwerte zusammen mit den in der .dll enthaltenen Lückentexten in die kompletten Ereignistexte umgesetzt. Dies erfolgt in der jeweils benutzten Systemsprache des SafeGuard Management Centers.

Die für die Ereignistexte verwendeten Lückentexte lassen sich, zum Beispiel durch SQL-Abfragen, bearbeiten und aufbereiten. Hierzu lässt sich eine Tabelle mit allen Lückentexten für die Ereignismeldungen erzeugen, die Sie dann Ihren spezifischen Anforderungen anpassen können.

So erstellen Sie eine Tabelle mit den Texten für die einzelnen Ereignis-IDs:

1. Wählen Sie in der Menüleiste des SafeGuard Management Centers **Extras** > **Optionen**.
2. Wechseln Sie im Fenster **Optionen** in die Registerkarte **Datenbank**.
3. Klicken Sie im Bereich **Texte für Ereignisberichte** auf die Schaltfläche **Erzeuge Tabelle**.

Die Tabelle mit den Texten für die Bericht IDs wird in der jeweils aktuellen Sprache des SafeGuard Management Centers erstellt und kann angepasst werden.

Achtung: Vor jedem neuen Erstellen der Lückentexte wird die Tabelle jeweils geleert. Wenn die Texte für eine Sprache wie beschrieben erstellt wurden und ein Benutzer erstellt die Texte für eine andere Sprache, so werden die Texte für die erste Sprache entfernt.

27 SafeGuard Enterprise und BitLocker-Laufwerkverschlüsselung

Die BitLocker-Laufwerkverschlüsselung ist ein in Microsoft Windows Vista und Windows 7 Betriebssysteme integriertes Feature für die Festplattenverschlüsselung mit Pre-Boot Authentication. BitLocker bietet Datenschutz durch die Verschlüsselung des Boot-Volumes.

27.1 Integration von BitLocker in SafeGuard Enterprise

In SafeGuard Enterprise lassen sich alle in einer Windows Vista, Windows 7 Enterprise oder Ultimate Installation verfügbaren BitLocker-Funktionen über das SafeGuard Management Center wie ein nativer SafeGuard Enterprise Client verwalten.

Während der Installation des SafeGuard Enterprise Client, muss die BitLocker-Unterstützung explizit ausgewählt werden, um die Integration von BitLocker zu ermöglichen.

Die zentrale und vollständig transparente Verwaltung von BitLocker durch SafeGuard Enterprise ermöglicht somit die Anwendung in heterogenen IT-Umgebungen. Neben der nahtlosen Integration von BitLocker bietet SafeGuard Enterprise jedoch auch eine erhebliche Aufwertung dieses Features. Über SafeGuard Enterprise lassen sich die Sicherheitsrichtlinien für BitLocker zentral ausrollen. Bei der Verwaltung von BitLocker über SafeGuard Enterprise stehen darüber hinaus äußerst wichtige Prozesse, wie Schlüsselverwaltung und Schlüssel-Recovery, zur Verfügung.

Für Informationen zur Unterstützung der BitLocker To Go Erweiterung in Windows 7 durch SafeGuard Enterprise, siehe *SafeGuard Enterprise und BitLocker To Go* auf Seite 308.

27.2 Aufwertung von BitLocker-Funktionalitäten mit SafeGuard Enterprise

Die Verwaltung von BitLocker mit SafeGuard Enterprise bietet Ihnen folgende Vorteile:

- Neben der Boot-Partition lassen sich auch weitere Volumes der lokalen Festplatte über die BitLocker-Verschlüsselung verschlüsseln.
- Zusätzlich lässt sich die dateibasierende Verschlüsselung von SafeGuard Enterprise auf alle Volumes anwenden, einschließlich Wechselmedien.
- Das SafeGuard Management Center ermöglicht die einfache Verwaltung von BitLocker Computern: Sicherheitsrichtlinien lassen sich aktualisieren, verteilen und automatisch anwenden.
- Der BitLocker-Verschlüsselungsstatus wird angezeigt.
- Sie können den BitLocker-Anmeldemodus definieren.

- Die Aktivierung sowie die Erstellung von Sicherungskopien von Schlüsseln wird im Vergleich zu nativen Vista-Umgebungen vereinfacht.
- Sowohl für Boot-Volumes als auch für andere Volumes steht ein BitLocker Recovery-Mechanismus für die Wiederherstellung von Passwörtern und Schlüsseldateien zur Verfügung.

27.3 Einsatz von SafeGuard Enterprise ohne BitLocker-Laufwerkverschlüsselung

Die volume-basierende Verschlüsselung mit SafeGuard Enterprise bietet im Vergleich zur BitLocker Laufwerkverschlüsselung eine Reihe von Vorteilen, z. B.:

- SafeGuard Enterprise unterstützt zusätzlich Windows XP und Vista Business.
  (BitLocker unterstützt lediglich Vista Enterprise und Ultimate.)
- Für die Installation ist keine spezifische Festplattenpartition erforderlich.
  (Für BitLocker ist eine eigene Partition erforderlich.)
- SafeGuard Enterprise unterstützt verschiedene Smartcards und Token für die Pre-Boot Authentisierung.
  (BitLocker unterstützt keine Smartcards sondern nur USB-Sticks, die eine kopierbare Schlüsseldatei enthalten.)
- SafeGuard Enterprise unterstützt mehrere verschiedene Benutzer und unterscheidet zwischen den einzelnen Benutzern in der Power-on Authentication.
  (BitLocker unterscheidet nicht zwischen verschiedenen Benutzern.)
- SafeGuard Enterprise bietet den sicheren, dynamischen Challenge/Response-Mechanismus zum Zurücksetzen vergessener Passwörter.
  (BitLocker verwendet einen festgelegten 48-stelligen Recovery-Schlüssel.)
- SafeGuard Enterprise bietet eine grafische Benutzeroberfläche in der Pre-Boot Authentisierung.
  (BitLocker bietet nur Text.)
- SafeGuard Enterprise akzeptiert komplexe Passwörter und Passwortregeln, die mit Windows synchronisiert sind.
  (Bei BitLocker ist nur eine TPM PIN zulässig.)
- SafeGuard Enterprise ermöglicht die sektorbasierende Verschlüsselung von Wechselmedien.
  (BitLocker verschlüsselt keine Wechselmedien. Wenn ein BitLocker-Client in Verbindung mit SafeGuard Enterprise verwendet wird, ist die dateibasierende Verschlüsselung von Wechselmedien möglich.)

27.4 BitLocker Clients mit SafeGuard Enterprise verwalten

Im SafeGuard Enterprise Management Center lassen sich BitLocker Endpoint-Computer wie andere native SafeGuard Endpoint-Computer verwalten. Als Sicherheitsbeauftragter können Sie Verschlüsselungs- und Authentisierungsrichtlinien für die BitLocker-Computer einrichten und verteilen.

Sobald ein BitLocker Endpoint-Computer bei SafeGuard Enterprise registriert ist, werden Informationen zu Benutzer, Computer, Anmeldemodus und Verschlüsselungsstatus angezeigt. Darüber hinaus werden Ereignisse für BitLocker Clients protokolliert.

Die Verwaltung von BitLocker Clients in SafeGuard Enterprise ist transparent. Das heißt, die Verwaltungsfunktionen haben im allgemeinen dieselbe Funktionsweise für BitLocker und native SafeGuard Enterprise Clients. Der Computertyp lässt sich in der Registerkarte **Bestand** eines Containers unter **Benutzer & Computer** ermitteln. Die Spalte **POA-Typ** zeigt an, ob es sich bei dem betreffenden Benutzer-PC um einen BitLocker Client oder einen nativen SafeGuard Enterprise Client handelt.

27.5 Verschlüsselung mit BitLocker über SafeGuard Enterprise

Mit der Unterstützung der BitLocker-Laufwerkverschlüsselung in SafeGuard Enterprise lassen sich die folgenden Komponenten verschlüsseln:

- Boot-Volume mit BitLocker-Verschlüsselung und BitLocker-Schlüsseln,
- andere Volumes mit BitLocker-Verschlüsselung und BitLocker-Schlüsseln,
- Daten, z. B. von Wechselmedien, mit SafeGuard Enterprise dateibasierender Verschlüsselung und SafeGuard Enterprise Schlüsseln.

Bitte beachten Sie, dass im Rahmen der SafeGuard Enterprise BitLocker-Unterstützung externe Festplatten als weitere Volumes und nicht als Wechselmedien behandelt werden. Sie können somit volume-basierend verschlüsselt werden.

27.5.1 BitLocker-Verschlüsselungsschlüssel

Bei der Verschlüsselung des Boot-Volumes oder anderer Volumes mit BitLocker über SafeGuard Enterprise werden die Verschlüsselungsschlüssel immer durch BitLocker erzeugt. BitLocker erzeugt jeweils einen Schlüssel für jedes Volume. Dieser Schlüssel lässt sich für keinen anderen Zweck verwenden und muss an einem sicheren Ort gespeichert werden.

Ein Vorteil der Anwendung von BitLocker in Verbindung mit SafeGuard Enterprise besteht hier darin, dass für jeden von BitLocker generierten Schlüssel eine Sicherungskopie des Schlüssels in der SafeGuard Enterprise Datenbank gespeichert wird. Dies ermöglicht die Einrichtung eines Helpdesk- und Recovery-Mechanismus (ähnlich der SafeGuard Enterprise Challenge/Response Funktionalität), der andernfalls in BitLocker nicht verfügbar wäre.

Es ist jedoch nicht möglich, Schlüssel global auszuwählen oder wiederzuverwenden, wie dies bei nativen SafeGuard Enterprise Clients der Fall ist. Die Schlüssel werden außerdem auch nicht im SafeGuard Management Center angezeigt.

Wenn vor der Installation der SafeGuard Enterprise BitLocker-Unterstützung bereits ein Volume mit BitLocker verschlüsselt wurde, muss der Systemadministrator Sicherungskopien von den Schlüsseln dieses Laufwerks über die von Microsoft zur Verfügung gestellten Sicherungsmechanismen erstellen.

Wenn ein Volume bei bereits installierter SafeGuard Enterprise BitLocker-Unterstützung verschlüsselt wird, kann der Systemverwalter die (mit einem Recovery-Kennwort gesicherten) Sicherungskopien der Schlüssel zusätzlich zum Speichern in der SafeGuard-Datenbank im Active Directory speichern. Dieser Vorgang muss manuell über das Windows Tool Manage BDE sowie durch Speichern der Schlüssel in einer Gruppenrichtlinie durchgeführt werden. Für Windows 2003 Server muss hierzu jedoch das verwendete Active Directory Schema erweitert werden. Darüber hinaus sind für die Wiederherstellung der Informationen Domänen-Administratorrechte erforderlich.

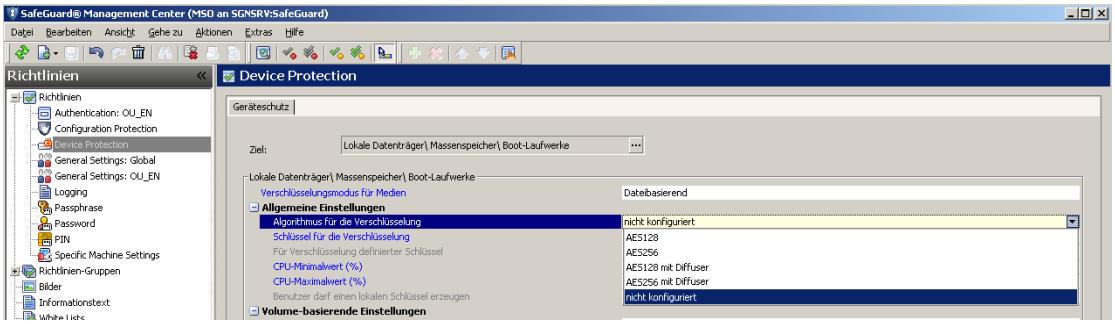
27.5.2 BitLocker-Algorithmen in SafeGuard Enterprise

BitLocker unterstützt die folgenden Advanced Encryption Standard (AES) Algorithmen:

- AES-128
- AES-256
- AES-128 mit Diffuser
- AES-256 mit Diffuser

Der Diffuser ist BitLocker-spezifisch und wird nicht für die volume-basierende Verschlüsselung von SafeGuard Enterprise verwendet. Wird ein Algorithmus mit Diffuser für die Verschlüsselung ausgewählt, verwenden alle nativen SafeGuard Enterprise Module den entsprechenden Algorithmustyp ohne Diffuser.

Wird sowohl den Computern mit BitLocker-Unterstützung als auch den nativen SafeGuard Enterprise Computern eine Richtlinie zugewiesen, so verwenden die nativen SafeGuard Enterprise Computer den Algorithmus ohne Diffuser und die BitLocker-Computer den Algorithmus mit Diffuser.



27.5.3 Verschlüsselungsrichtlinien für die BitLocker-Laufwerkverschlüsselung

Der Sicherheitsbeauftragte kann eine Richtlinie für die (Erst-)Verschlüsselung im SafeGuard Management Center anlegen und diese an die BitLocker Endpoint-Computer verteilen. Die Richtlinie wird daraufhin auf den Endpoint-Computern ausgeführt.

Da die BitLocker Clients im Management Center transparent verwaltet werden, muss der Sicherheitsbeauftragte keine speziellen BitLocker-Einstellungen für die Verschlüsselung vornehmen. SafeGuard Enterprise kennt den Status der Clients und wählt die BitLocker-Verschlüsselung entsprechend. Wird ein Bitlocker Client mit SafeGuard Enterprise installiert und wird die Volume-Verschlüsselung aktiviert, so werden die Volumes durch die BitLocker-Laufwerkverschlüsselung verschlüsselt.

27.6 Authentisierung mit BitLocker-Laufwerkverschlüsselung

Die BitLocker-Laufwerkverschlüsselung bietet eine Reihe von Optionen für die Authentisierung. BitLocker-Benutzer können sich entweder über ein Trusted Platform Module (TPM) oder einen USB-Stick oder über eine Kombination aus beidem authentisieren.

Der Sicherheitsbeauftragte kann die verschiedenen Anmeldemodi in einer Richtlinie im SafeGuard Management Center einstellen und sie an die BitLocker Endpoint-Computer verteilen.

Für SafeGuard Enterprise BitLocker-Benutzer sind folgende Anmeldemodi verfügbar:

- Nur TPM
- TPM + PIN
- TPM + USB Stick
- Nur USB Stick (ohne TPM)

Trusted Platform Module (TPM)

Das TPM ist ein Modul auf dem Motherboard, das einer Smartcard ähnelt und Verschlüsselungsfunktionen sowie Vorgänge für die digitale Signatur ausführt. Es ist in der Lage, Benutzerschlüssel anzulegen, zu speichern und zu verwalten. Das TPM ist gegen Angriffe geschützt.

USB-Stick

Die von BitLocker verwendeten Schlüssel können auf einem ungeschützten USB-Stick gespeichert werden.

27.7 Protokollierung

Vom BitLocker Client gemeldete Ereignisse werden wie für alle anderen SafeGuard Enterprise Clients protokolliert. Dabei wird nicht explizit erwähnt, dass sich das Ereignis auf einen BitLocker Client bezieht. Die Berichte entsprechen den für jeden anderen SafeGuard Enterprise Client erzeugten Berichten.

28 SafeGuard Enterprise und BitLocker To Go

Mit BitLocker To Go wurde in Microsoft Windows 7 die BitLocker-Laufwerkverschlüsselung erweitert. BitLocker unterstützt nun die Verschlüsselung von internen Volumes und von Wechseldatenträgern auf Endpoint-Computern über das Windows Explorer Kontextmenü.

- Wenn der native SafeGuard Enterprise Device Encryption Client mit aktivierter „BitLocker-Unterstützung“ installiert wurde, wird BitLocker To Go unterstützt.
- Wenn der SafeGuard Enterprise Device Encryption Client ohne aktivierte „BitLocker-Unterstützung“ installiert wurde, oder wenn der SafeGuard Data Exchange Client installiert wurde, ist die Verschlüsselung über BitLocker To Go nicht kompatibel. Sie muss in diesem Fall deaktiviert werden. Die Verschlüsselung von internen Volumes und von Wechseldatenträgern kann jedoch zentral und komfortabel über SafeGuard Enterprise Sicherheitsrichtlinien konfiguriert werden. Interne Volumes und Wechseldatenträger, die bereits vor dem Einsatz des SafeGuard Enterprise Device Encryption Clients mit BitLocker To Go verschlüsselt wurden, bleiben weiterhin lesbar.

Gehen Sie folgendermaßen vor, um die BitLocker To Go Verschlüsselung zu deaktivieren:

1. Wählen Sie im Windows Gruppenrichtlinienverwaltungs-Editor **Default Domain Policy** > **Computerkonfiguration** > **Richtlinien** > **Administrative Vorlagen** (**lokaler Computer**)> **Windows-Komponenten** > **BitLocker Laufwerkverschlüsselung** > **Wechseldatenträger**.
2. Unter **Wechseldatenträger** wählen Sie die folgende Richtlinie: **Verwendung von BitLocker auf Wechseldatenträgern steuern**. Setzen Sie die Optionen wie folgt:
   - Wählen Sie **Aktiviert**.
   - Unter **Optionen** deaktivieren Sie: **Benutzer können BitLocker-Schutz auf Wechseldatenträgern anwenden**.
   - Unter **Optionen** aktivieren Sie: **Benutzer können BitLocker-Schutz auf Wechseldatenträgern anhalten und entschlüsseln**.
3. Bestätigen Sie mit **OK**.

BitLocker To Go Verschlüsselung wird auf den Endpoint-Computern deaktiviert. Der Benutzer kann neue Laufwerke nicht mehr mit BitLocker To Go verschlüsseln. Laufwerke, die bereits vor dem Betrieb des nativen SafeGuard Enterprise Device Encryption Client mit BitLocker To Go verschlüsselt wurden, bleiben lesbar.

Die Registry-Einstellungen werden folgendermaßen gesetzt:

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE]

"RDVConfigureBDE"=dword:00000001

"RDVAllowBDE"=dword:00000000

"RDVDisableBDE"=dword:00000001

29 Für Berichte auswählbare Ereignisse

Die folgende Tabelle bietet einen Überblick zu allen für die Protokollierung auswählbaren Ereignissen.

Kategorie	Ereignis-ID	Beschreibung
System	1005	Dienst gestartet.
System	1006	Dienst starten fehlgeschlagen
System	1007	Dienst angehalten.
System	1016	Integritätstest der Dateien fehlgeschlagen.
System	1017	Logging Ziel nicht verfügbar.
System	1018	Nicht genehmigter Versuch SafeGuard Enterprise zu deinstallieren
Anmeldung	2001	Externe GINA erkannt und erfolgreich eingebunden.
Anmeldung	2002	Externe GINA erkannt, Einbindung fehlgeschlagen.
Anmeldung	2003	Power-on Authentication ist aktiviert.
Anmeldung	2004	Power-on Authentication ist deaktiviert.
Anmeldung	2005	Wake on LAN ist aktiviert.
Anmeldung	2006	Wake on LAN ist deaktiviert.
Anmeldung	2007	Challenge erzeugt.
Anmeldung	2008	Response erzeugt.
Anmeldung	2009	Anmeldung erfolgreich durchgeführt.
Anmeldung	2010	Anmeldung fehlgeschlagen.
Anmeldung	2011	Benutzer während Anmeldung importiert und als Besitzer markiert.
Anmeldung	2012	Benutzer vom Besitzer importiert und als Nicht- Besitzer markiert
Anmeldung	2013	Benutzer von Nicht-Besitzer importiert und als Nicht-Besitzer markiert.
Anmeldung	2014	Benutzer als Besitzer entfernt.
Anmeldung	2015	Import des Benutzers während der Anmeldung fehlgeschlagen.
Anmeldung	2016	Benutzer hat sich abgemeldet.
Anmeldung	2017	Benutzer wurde zwangsweise abgemeldet.

Kategorie	Ereignis-ID	Beschreibung
Anmeldung	2018	Aktion wurde auf dem Gerät ausgeführt.
Anmeldung	2019	Benutzer hat einen Kennwort/PIN-Wechsel eingeleitet.
Anmeldung	2020	Der Benutzer hat nach der Anmeldung sein Kennwort/ PIN geändert.
Anmeldung	2021	Kennwort/PIN-Qualität.
Anmeldung	2022	Der Kennwort/PIN-Wechsel konnte nicht durchgeführt werden.
Anmeldung	2023	Der LocalCache war korrupt und wurde restauriert
Anmeldung	2024	Ungültige Passwort Blacklist Konfiguration
Anmeldung	2025	Der empfangene Response Code erlaubt es dem Benutzer, sich sein Passwort anzeigen zu lassen.
Anmeldung	2071	Kernel-Initialisierung wurde erfolgreich beendet.
Anmeldung	2072	Kernel-Initialisierung ist fehlgeschlagen.
Anmeldung	2073	Maschinenschlüssel wurden erfolgreich zum Server gesendet.
Anmeldung	2074	Maschinenschlüssel konnten nicht erfolgreich zum Server gesendet werden.
Anmeldung	2079	Import eines Benutzers in den Kernel wurde erfolgreich beendet.
Anmeldung	2080	Löschen eines Benutzers aus dem Kernel wurde erfolgreich beendet.
Anmeldung	2081	Import eines Benutzers in den Kernel ist fehlgeschlagen.
Anmeldung	2082	Löschen eines Benutzers aus dem Kernel ist fehlgeschlagen.
Anmeldung	2083	Response mit Aktion "Benutzer wird sein Kennwort angezeigt" erzeugt.
Anmeldung	2084	Response für virtuellen Client erzeugt.
Anmeldung	2085	Response für Standalone Client erzeugt.
Anmeldung	2095	Wake on LAN konnte nicht aktiviert werden.
Anmeldung	2096	Wake on LAN konnte nicht deaktiviert werden.
Administration	2500	SafeGuard Enterprise Administration gestartet.
Administration	2501	Anmeldung an der SafeGuard Enterprise Administration fehlgeschlagen

Kategorie	Ereignis-ID	Beschreibung
Administration	2502	Autorisierung an der SafeGuard Enterprise Administration fehlgeschlagen.
Administration	2504	Benutzer genehmigt zusätzliche Autorisierung
Administration	2505	Zusätzliche Autorisierung von Benutzer fehlgeschlagen.
Administration	2506	Datenimport vom Verzeichnis erfolgreich.
Administration	2507	Datenimport vom Verzeichnis abgebrochen.
Administration	2508	Datenimport vom Verzeichnis fehlgeschlagen.
Administration	2511	Benutzer angelegt.
Administration	2513	Benutzer wurde geändert.
Administration	2515	Benutzer gelöscht.
Administration	2518	Anlegen des Benutzers fehlgeschlagen.
Administration	2522	Löschen des Benutzers fehlgeschlagen.
Administration	2525	Computer angelegt
Administration	2529	Computer gelöscht.
Administration	2532	Anlegen des Computers fehlgeschlagen.
Administration	2536	Löschen des Computers fehlgeschlagen.
Administration	2539	OU angelegt.
Administration	2543	OU gelöscht.
Administration	2546	Anlegen der OU fehlgeschlagen
Administration	2547	Importieren der OU fehlgeschlagen.
Administration	2550	Löschen der OU fehlgeschlagen.
Administration	2553	Gruppe angelegt.
Administration	2555	Gruppe geändert.
Administration	2556	Gruppe umbenannt.
Administration	2557	Gruppe gelöscht.
Administration	2560	Anlegen der Gruppe fehlgeschlagen.
Administration	2562	Ändern der Gruppe fehlgeschlagen.
Administration	2563	Umbenennen der Gruppe fehlgeschlagen.
Administration	2564	Löschen der Gruppe fehlgeschlagen.
Administration	2573	Mitglieder der Gruppe hinzugefügt.

Kategorie	Ereignis-ID	Beschreibung
Administration	2575	Mitglieder aus Gruppe entfernt.
Administration	2576	Hinzufügen der Mitglieder zur Gruppe fehlgeschlagen.
Administration	2578	Entfernen der Mitglieder aus Gruppe fehlgeschlagen.
Administration	2580	Gruppe von OU nach OU verschoben.
Administration	2583	Verschieben der Gruppe von OU nach OU fehlgeschlagen.
Administration	2591	Objekte der Gruppe hinzugefügt.
Administration	2593	Objekte aus Gruppe entfernt.
Administration	2594	Hinzufügen der Objekte zur Gruppe fehlgeschlagen
Administration	2596	Hinzufügen der Objekte aus Gruppe fehlgeschlagen
Administration	2603	Schlüssel erzeugt. Algorithmus.
Administration	2607	Schlüssel zugeordnet.
Administration	2608	Schlüsselzuordnung aufgehoben.
Administration	2609	Erzeugen des Schlüssels fehlgeschlagen.
Administration	2613	Zuordnung des Schlüssels fehlgeschlagen.
Administration	2614	Entfernen der Zuordnung des Schlüssels fehlgeschlagen.
Administration	2615	Zertifikat erzeugt.
Administration	2616	Zertifikat importiert.
Administration	2619	Zertifikat gelöscht.
Administration	2621	Zertifikat Benutzer zugeordnet.
Administration	2622	Zertifikatszuordnung zu Benutzer aufgehoben.
Administration	2623	Erzeugen des Zertifikats fehlgeschlagen.
Administration	2624	Importieren des Zertifikats fehlgeschlagen.
Administration	2627	Löschen des Zertifikats fehlgeschlagen.
Administration	2628	Verlängern des Zertifikats fehlgeschlagen.
Administration	2629	Zuordnen des Zertifikats zu Benutzer fehlgeschlagen.
Administration	2630	Entfernen der Zuordnung des Zertifikats vom Benutzer fehlgeschlagen.
Administration	2631	Token eingesteckt.
Administration	2632	Token entfernt.
Administration	2633	Token wurde für Benutzer ausgestellt.

Kategorie	Ereignis-ID	Beschreibung
Administration	2634	PIN des Benutzers auf Token ändern.
Administration	2635	PIN des Sicherheitsbeauftragten auf Token ändern.
Administration	2636	Token wurde gesperrt.
Administration	2637	Token entsperrt.
Administration	2638	Token gelöscht.
Administration	2639	Tokenzuordnung für Benutzer aufgehoben.
Administration	2640	Ausstellen des Tokens für Benutzer fehlgeschlagen.
Administration	2641	Ändern der Benutzer-PIN auf Token fehlgeschlagen.
Administration	2642	Ändern der Sicherheitsbeauftragten-PIN auf Token fehlgeschlagen.
Administration	2643	Sperren des Tokens fehlgeschlagen.
Administration	2644	Entsperren des Tokens fehlgeschlagen.
Administration	2645	Löschen des Tokens fehlgeschlagen.
Administration	2647	Richtlinie erstellt.
Administration	2648	Richtlinie geändert.
Administration	2650	Richtlinie gelöscht.
Administration	2651	Richtlinie der OU zugewiesen und aktiviert.
Administration	2652	Zugewiesene Richtlinie wurde von OU entfernt.
Administration	2653	Erstellen der Richtlinie fehlgeschlagen.
Administration	2654	Ändern der Richtlinie fehlgeschlagen.
Administration	2657	Zuweisung und Aktivierung der Richtlinie zu OU fehlgeschlagen.
Administration	2658	Entfernen der zugewiesenen Richtlinie von OU ist fehlgeschlagen.
Administration	2659	Richtlinien-Gruppe angelegt.
Administration	2660	Richtlinien-Gruppe geändert.
Administration	2661	Richtlinien-Gruppe gelöscht.
Administration	2662	Anlegen der Richtlinien-Gruppe fehlgeschlagen.
Administration	2663	Ändern der Richtlinien-Gruppe fehlgeschlagen.
Administration	2665	Folgende Richtlinie wurde der Richtlinien-Gruppe hinzugefügt.

Kategorie	Ereignis-ID	Beschreibung
Administration	2667	Folgende Richtlinie wurde aus der Richtlinien-Gruppe entfernt.
Administration	2668	Hinzufügen der Richtlinie zur Richtlinien-Gruppe fehlgeschlagen.
Administration	2670	Entfernen der Richtlinie aus Richtlinien-Gruppe fehlgeschlagen.
Administration	2678	Protokollierte Ereignisse exportiert.
Administration	2679	Exportieren der protokollierten Ereignisse fehlgeschlagen.
Administration	2680	Protokollierte Ereignisse gelöscht.
Administration	2681	Löschen der protokollierten Ereignisse fehlgeschlagen.
Administration	2684	Sicherheitsbeauftragter erlaubt die Erneuerung eines Zertifikats
Administration	2685	Beauftragter verbietet die Erneuerung eines Zertifikats
Administration	2686	Änderungen an den Einstellungen für die Zertifikatserneuerung fehlgeschlagen
Administration	2687	Zertifikat für Beauftragten gewechselt
Administration	2688	Zertifikatswechsel für Beauftragten fehlgeschlagen
Administration	2692	Erzeugen von Arbeitsgruppen.
Administration	2693	Fehlgeschlagenes Erzeugen von Arbeitsgruppen
Administration	2694	Löschen von Arbeitsgruppen.
Administration	2695	Fehlgeschlagenes Löschen von Arbeitsgruppen
Administration	2696	Erzeugen von Benutzern.
Administration	2697	Fehlgeschlagenes Erzeugen von Benutzern.
Administration	2698	Erzeugen von Maschinen.
Administration	2699	Fehlgeschlagenes Erzeugen von Maschinen.
Administration	2700	Die Lizenz wurde verletzt.
Administration	2701	Schlüsseldatei wurde erzeugt.
Administration	2702	Schlüssel für Schlüsseldatei wurde gelöscht.
Administration	2703	Sicherheitsbeauftragter hat die Power-on Authentication in einer Richtlinie deaktiviert.
Client	3003	Kernelsicherung erfolgreich
Client	3005	Kernelrücksicherung beim ersten Versuch erfolgreich

Kategorie	Ereignis-ID	Beschreibung
Client	3006	Kernelrücksicherung beim zweiten Versuch erfolgreich
Client	3007	Kernelsicherung fehlgeschlagen
Client	3008	Kernelrücksicherung fehlgeschlagen
Client	3405	Deinstallation des Configuration Protection Clients fehlgeschlagen.
Client	3406	Interner Fehler im Configuration Protection Client
Client	3407	Möglicher Manipulationsvorgang vom Configuration Protection Client festgestellt.
Client	3408	Möglicher Manipulationsvorgang am Ereignisprotokoll des Configuration Protection Clients.
Verschlüsselung	3501	Zugriff auf Medium im Laufwerk verweigert.
Verschlüsselung	3502	Zugriff auf Datei verweigert.
Verschlüsselung	3503	Sektorbasierte Erst-Verschlüsselung des Laufwerks gestartet.
Verschlüsselung	3504	Sektorbasierte Erst-Verschlüsselung des Laufwerks gestartet. (Schnellmodus).
Verschlüsselung	3505	Sektorbasierte Erst-Verschlüsselung des Laufwerks fehlerfrei beendet.
Verschlüsselung	3506	Sektorbasierte Erst-Verschlüsselung des Laufwerks gescheitert und beendet.
Verschlüsselung	3507	Sektorbasierte Erst-Verschlüsselung des Laufwerks abgebrochen.
Verschlüsselung	3508	Sektorbasierte Erst-Verschlüsselung des Laufwerks fehlgeschlagen.
Verschlüsselung	3509	Sektorbasierte Entschlüsselung des Laufwerks gestartet.
Verschlüsselung	3510	Sektorbasierte Entschlüsselung des Laufwerks fehlerfrei beendet.
Verschlüsselung	3511	Sektorbasierte Entschlüsselung des Laufwerks gescheitert und beendet.
Verschlüsselung	3512	Sektorbasierte Entschlüsselung des Laufwerks abgebrochen.
Verschlüsselung	3513	Sektorbasierte Entschlüsselung des Laufwerks fehlgeschlagen.
Verschlüsselung	3514	F&F Erst-Verschlüsselung auf einem Laufwerk gestartet.

Kategorie	Ereignis-ID	Beschreibung
Verschlüsselung	3515	F&F Erst-Verschlüsselung auf einem Laufwerk fehlerfrei beendet.
Verschlüsselung	3516	F&F Erst-Verschlüsselung auf einem Laufwerk fehlgeschlagen und beendet.
Verschlüsselung	3517	F&F Erst-Verschlüsselung auf einem Laufwerk abgebrochen.
Verschlüsselung	3519	F&F Entschlüsselung auf einem Laufwerk gestartet.
Verschlüsselung	3520	F&F Entschlüsselung auf einem Laufwerk fehlerfrei beendet.
Verschlüsselung	3521	F&F Entschlüsselung auf einem Laufwerk fehlgeschlagen und beendet.
Verschlüsselung	3522	F&F Entschlüsselung auf einem Laufwerk abgebrochen.
Verschlüsselung	3524	F&F Verschlüsselung einer Datei gestartet.
Verschlüsselung	3525	F&F Verschlüsselung einer Datei fehlerfrei beendet.
Verschlüsselung	3526	F&F Verschlüsselung einer Datei fehlgeschlagen.
Verschlüsselung	3540	F&F-Entschlüsselung einer Datei gestartet.
Verschlüsselung	3541	F&F-Entschlüsselung einer Datei fehlerfrei beendet.
Verschlüsselung	3542	F&F-Entschlüsselung einer Datei fehlgeschlagen.
Verschlüsselung	3543	Backup von Bootkey durchgeführt
Verschlüsselung	3544	Überschreitung der Anzahl von Verschlüsselungsalgorithmen für Start-Laufwerke
Verschlüsselung	3545	Lesefehler von Schlüsseldatenbereiche
Verschlüsselung	3546	Abweisen von Laufwerken gemäß den Richtlinien.
Verschlüsselung	3560	Zugriffsschutz
Verschlüsselung	3600	Allgemeiner Verschlüsselungsfehler
Verschlüsselung	3601	Verschlüsselungsfehler - Laufwerk nicht gefunden
Verschlüsselung	3602	Verschlüsselungsfehler - Laufwerk nicht verfügbar
Verschlüsselung	3603	Verschlüsselungsfehler - Laufwerk entfernt
Verschlüsselung	3604	Verschlüsselungsfehler - Laufwerksfehler
Verschlüsselung	3607	Verschlüsselungsfehler - Der Schlüssel fehlt
Verschlüsselung	3610	Verschlüsselungsfehler - Der Original-KSA Bereich ist beschädigt.

Kategorie	Ereignis-ID	Beschreibung
Verschlüsselung	3611	Verschlüsselungsfehler - Der Sicherungs-KSA Bereich ist beschädigt.
Verschlüsselung	3612	Verschlüsselungsfehler - Der ESA-Bereich ist beschädigt.
Zugriffskontrolle	4400	Port erfolgreich freigegeben
Zugriffskontrolle	4401	Gerät erfolgreich freigegeben
Zugriffskontrolle	4402	Speichergerät erfolgreich freigegeben
Zugriffskontrolle	4403	WLAN erfolgreich freigegeben
Zugriffskontrolle	4404	Port erfolgreich entfernt
Zugriffskontrolle	4405	Gerät erfolgreich entfernt
Zugriffskontrolle	4406	Speichergerät erfolgreich entfernt
Zugriffskontrolle	4407	WLAN-Verbindung erfolgreich getrennt
Zugriffskontrolle	4408	Port eingeschränkt
Zugriffskontrolle	4409	Gerät eingeschränkt
Zugriffskontrolle	4410	Speichergerät eingeschränkt
Zugriffskontrolle	4411	WLAN eingeschränkt
Zugriffskontrolle	4412	Port gesperrt
Zugriffskontrolle	4413	Gerät gesperrt
Zugriffskontrolle	4414	Speichergerät gesperrt
Zugriffskontrolle	4415	WLAN gesperrt

30 Bedeutung der SGMERR-Codes in der Windows-Ereignisanzeige

In der Windows-Ereignisanzeige könnten Sie folgende Meldung finden:

“Authorization for SafeGuard Enterprise Administration failed for user.... Reason: [536870951]”

Welche Bedeutung die Nummer “536870951” hat, finden Sie in dieser Tabelle. Nummer “536870951” bedeutet zum Beispiel “Die angegebene PIN ist falsch, der Benutzer konnte nicht authentisiert werden”.

Fehler-ID	Anzeige
0	OK
1	Fehler in Parameter 1
2	Fehler in Parameter 2
3	Fehler in Parameter 3
4	Fehler in Parameter 4
5	Fehler in Parameter 5
6	Fehler in Parameter 6
7	Fehler in Parameter 7
8	Fehler in Parameter 8
9	Fehler in Parameter 9
10	Fehler in Parameter 10
11	Fehler in Parameter 11
12	Fehler in Parameter 12
13	Fehler in Parameter 13
14	Fehler in Parameter 14
15	Fehler in Parameter 15
16	Fehler in Parameter 16
17	Fehler in Parameter 17
18	Fehler in Parameter 18
19	Fehler in Parameter 19
20	Funktion nicht ausgeführt
21	Interner Fehler entdeckt

22	Modul nicht initialisiert
23	Datei I/O Fehler entdeckt
24	Speicher kann nicht zugewiesen werden
25	Datei I/O Lesefehler
26	Datei I/O Schreibfehler
50	Keine Operation durchgeführt
101	Allgemeiner Fehler
102	Zugriff verweigert
103	Datei existiert bereits
1201	Registry Eintrag konnte nicht geöffnet werden.
1202	Registry Eintrag konnte nicht gelesen werden.
1203	Registry Eintrag konnte nicht geschrieben werden.
1204	Registry Eintrag konnte nicht entfernt werden.
1205	Registry Eintrag konnte nicht erzeugt werden.
1206	Kein Zugriff auf einen Systemdienst oder Treiber möglich.
1207	Ein Systemdienst oder Treiber konnte nicht in der Registry eingetragen werden.
1208	Ein Systemdienst oder Treiber konnte nicht aus der Registry entfernt werden.
1209	Ein Systemdienst oder Treiber ist bereits in der Registry eingetragen.
1210	Kein Zugriff auf den Service Control Manager möglich.
1211	Ein Eintrag für eine Session konnte in der Registry nicht gefunden werden.
1212	Ein Registry Eintrag is ungültig oder falsch.
1301	Zugriff auf ein Laufwerk ist fehlgeschlagen.
1302	Keine Informationen über ein Laufwerk vorhanden.
1303	Kein Zugriff auf ein Volume möglich.
1304	Ungültige Option definiert.
1305	Unzulässiges Dateisystem.
1306	Das existierende Dateisystem auf einem Volume und das definierte sind unterschiedlich.
1307	Die vorhandene Größe eines Dateisystem-Clusters und die definierte Größe sind unterschiedlich.
1308	Unzulässige Sektorgröße eines Dateisystems definiert.

1309	Unzulässiger Startsektor definiert.
1310	Unzulässiger Partitionstyp definiert.
1311	Es konnte kein unfragmentierter, unbenutzer Bereich der erforderlichen Größe auf einem Volume gefunden werden.
1312	Dateisystem Cluster konnten nicht als benutzt markiert werden.
1313	Dateisystem Cluster konnten nicht als GOOD markiert werden.
1314	Dateisystem Cluster konnten nicht als unbenutzt markiert werden.
1315	Dateisystem Cluster konnten nicht als BAD markiert werden.
1316	Es existieren keine Informationen über die Cluster eines Dateisystems.
1317	Der als BAD markierte Bereich auf einem Volume konnte nicht gefunden werden.
1318	Unzulässige Größe eines Bereichs auf einem Volume definiert.
1319	Der MBR Sektor einer Festplatte konnte nicht ersetzt werden.
1330	Ein falsches Kommando für eine Allokierung oder Deallokierung definiert.
1351	Unzulässiger Algorithmus definiert.
1352	Der Zugriff auf den Systemkern ist fehlgeschlagen.
1353	Es ist kein Systemkern installiert.
1354	Beim Zugriff auf den Systemkern ist ein Fehler aufgetreten.
1355	Unzulässige Änderung der Systemeinstellungen.
1401	Auf ein Laufwerk konnten keine Daten geschrieben werden.
1402	Von einem Laufwerk konnten keine Daten gelesen werden.
1403	Der Zugriff auf ein Laufwerk ist fehlgeschlagen.
1404	Unzulässiges Laufwerk.
1405	Änderung der Zugriffsposition auf einem Laufwerk ist fehlgeschlagen.
1406	Laufwerk ist nicht bereit.
1407	Unmount eines Laufwerks ist fehlgeschlagen.
1451	Datei konnte nicht geöffnet werden.
1452	Datei konnte nicht gefunden werden.
1453	Unzulässiger Dateipfad definiert.
1454	Datei konnte nicht erzeugt werden.
1455	Datei konnte nicht kopiert werden.
1456	Keine Informationen über ein Laufwerk vorhanden.

1457	Die Position in einer Datei konnte nicht geändert werden.
1458	Das Lesen von einer Datei ist fehlgeschlagen.
1459	Es konnten keine Daten in eine Datei geschrieben werden.
1460	Eine Datei konnte nicht entfernt werden.
1461	Unzulässiges Dateisystem.
1462	Datei konnte nicht geschlossen werden.
1463	Kein Zugriff auf eine Datei möglich.
1501	Nicht genug Speicher vorhanden.
1502	Unzulässiger oder falscher Parameter definiert.
1503	Ein Puffer für Daten ist zu klein.
1504	Ein DLL-Modul konnte nicht geladen werden.
1505	Eine Funktion oder ein Prozess wurde abgebrochen.
1506	Kein Zugriff erlaubt.
1510	Es ist kein Systemkern installiert.
1511	Ein Programm konnte nicht gestartet werden.
1512	Eine Funktion, ein Objekt oder Daten sind nicht vorhanden.
1513	Unzulässiger Eintrag.
1514	Ein Objekt existiert bereits.
1515	Unzulässiger Funktionsaufruf.
1516	Es ist ein interner Fehler aufgetreten.
1517	Es ist eine Zugriffsverletzung aufgetreten.
1518	Funktion oder Modus wird nicht unterstützt.
1519	Deinstallation ist fehlgeschlagen.
1520	Es ist ein Ausnahmefehler aufgetreten.
1550	Der MBR Sektor der Festplatte konnte nicht ersetzt werden.
20001	Unbekannt
20002	Prozess beendet
20003	Datei nicht verifiziert
20004	Ungültige Richtlinie
30050	Die Anweisung Öffnen war nicht erfolgreich
30051	Nicht genug Speicherplatz

30052	Allgemeiner Fehler in der Prozess-Kommunikation
30053	Auf eine Resource kann nicht zugegriffen werden. Das ist ein temporärer Zustand und ein späterer Versuch könnte erfolgreich beendet werden.
30054	Allgemeiner Kommunikationsfehler
30055	Unerwarteter Rückgabewert
30056	Kein Kartenlesegrät angeschlossen
30057	Zwischenspeicher überfüllt
30058	Karte ist nicht in Betrieb
30059	Eine Zeitüberschreitung ist eingetreten
30060	Unerlaubter Kartentyp
30061	Die gewünschte Funktionsart wird nicht unterstützt /zu dieser Zeit / In dieser OS / in dieser Situation.
30062	Ungültiger Treiber
30063	Die Firmware der angeschlossenen Hardware ist von dieser Software nicht nutzbar
30064	Öffnen der Datei ist fehlgeschlagen
30065	Datei nicht gefunden
30066	Karte nicht eingeführt
30067	Unzulässiges Argument
30068	Die Semaphore wird derzeit verwendet.
30069	Die Semaphore ist momentan in Benutzung
30070	Allgemeiner Fehler.
30071	Sie haben momentan nicht die Rechte, die angefragte Aktion durchzuführen. Normalerweise ist es notwendig zuvor ein Kennwort einzugeben.
30072	Der Service ist momentan nicht verfügbar.
30073	Ein Element (z. B. ein Schlüssel mit einem bestimmten Namen) konnte nicht gefunden werden.
30074	Das angegebene Kennwort ist falsch.
30075	Das Kennwort wurde mehrere Male falsch eingegeben und ist daher geblockt. Benutzen Sie ein Verwaltungstool, um dieses zu entsperren.
30076	Die Identität stimmt nicht mit der definierten Identitäts-Gegenprobe überein.

30077	Mehrere Fehler sind aufgetreten. Benutzen sie diesen Fehlercode, wenn dies die einzige Möglichkeit ist, einen Fehlercode zu erhalten, aber vorher verschiedene Fehler aufgetreten sind.
30078	Einige Elemente sind noch vorhanden, daher kann z. B. die Verzeichnisstruktur etc. nicht gelöscht werden.
30079	Fehler während des Konsistenztestes
30080	Die ID ist auf der Schwarzen Liste. Die angefragte Aktion ist daher nicht erlaubt.
30081	Ungültiges Handle
30082	Ungültige Konfigurationsdatei
30083	Abschnitt nicht gefunden.
30084	Eintrag nicht gefunden.
30085	Keine weiteren Abschnitte vorhanden.
30086	Ende der Datei erreicht.
30087	Der angegebene Element existiert bereits.
30088	Das Kennwort ist zu kurz.
30089	Das Kennwort ist zu lang.
30090	Ein Element (z. B. ein Zertifikat) ist abgelaufen.
30091	Das Kennwort ist nicht gesperrt.
30092	Der Pfad konnte nicht gefunden werden.
30093	Das Datenverzeichnis ist nicht leer.
30094	Keine weiteren Daten verfügbar
30095	Auf dem Medium ist kein Speicherplatz mehr verfügbar.
30096	Eine Operation wurde abgebrochen.
30097	Read Only Daten; eine Schreiboperation ist fehlgeschlagen.
12451841	Der Schlüssel ist nicht verfügbar.
12451842	Der Schlüssel ist nicht definiert.
12451843	Zugriff auf unverschlüsseltes Medium verweigert.
12451844	Zugriff auf unverschlüsseltes Medium verweigert, wenn nicht es nicht leer ist.
352321637	Die Datei ist nicht verschlüsselt.
352321638	Der Schlüssel ist nicht verfügbar.
352321639	Der richtige Schlüssel ist nicht verfügbar.

352321640	Checksummenfehler im Datei-Header.
352321641	Fehler in CBI-Funktion.
352321642	Ungültiger Dateiname.
352321643	Fehler beim Lesen/Schreiben der temporären Datei.
352321644	Zugriff auf unverschlüsselte Dateien ist nicht erlaubt.
352321645	Key Storage Area (KSA) voll.
352321646	Die Datei ist bereits mit einem anderen Algorithmus verschlüsselt.
352321647	Datei ist mit NTFS komprimiert und kann daher nicht verschlüsselt werden!
352321648	Datei ist mit EFS verschlüsselt!
352321649	Ungültiger Datei-Besitzer!
352321650	Ungültiger Dateiverschlüsselungsmodus!
352321651	Fehler im CBC-Handling!
385875969	Integrität verletzt.
402653185	Das Token enthält keine Berechtigungen.
402653186	Berechtigungen können nicht auf das Token geschrieben werden.
402653187	TDF-Tag konnte nicht angelegt werden.
402653188	TDF-Tag enthält die angeforderten Daten nicht.
402653189	Das Objekt existiert bereits auf dem Token.
402653190	Kein gültiger Slot gefunden.
402653191	Seriennummer konnte nicht gelesen werden
402653192	Verschlüsselung des Tokens ist gescheitert.
402653193	Entschlüsselung des Tokens ist gescheitert.
536870913	Die Schlüsseldatei enthält eine ungültige Daten.
536870914	Teile des RSA-Schlüsselpaares sind ungültig.
536870915	Das Schlüsselpaar konnte nicht importiert werden.
536870916	Das Format der Schlüsseldatei ist ungültig.
536870917	Keine Daten verfügbar.
536870918	Der Import des Zertifikates ist fehlgeschlagen, da das Zertifikat bereits exsitiert..
536870919	Das Modul ist bereits initialisiert worden.
536870920	Das Modul ist nicht initialisiert worden.

536870921	Die ASN.1-Verschlüsselung ist fehlerhaft.
536870922	Fehlerhafte Datenlänge.
536870923	Fehlerhafte Signatur.
536870924	Fehlerhafter Verschlüsselungsmechanismus angewandt.
536870925	Diese Version wird nicht unterstützt.
536870926	Padding Fehler.
536870927	Ungültige Flags.
536870928	Das Zertifikat ist abgelaufen und nicht länger gültig.
536870929	Unkorrekte Zeitangabe. Zertifikat noch nicht gültig.
536870930	Das Zertifikat ist entzogen worden.
536870931	Die Zertifikats-Kette ist ungültig.
536870932	Die Zertifikats-Kette konnte nicht erstellt werden.
536870933	CDP konnte nicht kontaktiert werden.
536870934	Ein Zertifikat, welches nur als End-Dateneinheit genutzt werden kann, ist als CA oder umgekehrt genutzt worden.
536870935	Probleme mit der Gültigkeitslänge der Zertifikate in der Kette.
536870936	Fehler bei der Öffnung der Datei.
536870937	Fehler beim Lesen einer Datei.
536870938	Ein oder mehrere Parameter, die an die Funktion übergeben worden sind, sind nicht korrekt.
536870939	Die Ausgabe der Funktion passt nicht in den zur Verfügung gestellten Puffer.
536870940	Ein Problem mit dem Token und/oder Slot ist aufgetaucht.
536870941	Der Token hat nicht genug Speicherkapazität, um die gewünschte Funktion auszuführen.
536870942	Der Token ist aus dem Slot entfernt worden, während die Funktion ausgeführt wurde.
536870943	Die gewünschte Funktion konnte nicht ausgeführt werden, es liegen aber keine detaillierten Informationen über den Grund der Fehlermeldung vor.
536870944	Ein allgemeiner Fehler ist aufgetreten. Das System könnte instabil sein.
536870945	Der Computer auf dem die CBI Sammlung läuft, besitzt ungenügenden Speicher, um die gewünschte Funktion auszuführen. Im schlechtesten Fall könnte es sein, dass die Funktion nur teilweise erfolgreich durchgeführt wird.

536870946	Eine gewünschte Funktion wird nicht vom CBI-Archiv unterstütz.
536870947	Es wurde versucht, einen Wert für ein Objekt einzustellen, welches nicht eingestellt oder abgeändert werden kann.
536870948	Ein ungültiger Wert wurde für ein Objekt angegeben.
536870949	Es wurde versucht, den Wert eines Objektes zu erlangen, was jedoch fehlschlug, da es sich um ein sensibles Objekt handelt bzw. es nicht extrahierbar ist.
536870950	Die angegebene OIN Lust abgelaufen. (Ob eine PIN eines normalen Benutzers auf einem ausgegebenen Token jemals abläuft, variiert von Token zu Token.)
536870951	Die angegebene PIN ist falsch, der Benutzer konnte nicht authentisiert werden.
536870952	Die angegebene PIN enthält ungültige Zeichen. Dieser Antwort-Code wird nur für Funktionen angewandt, die versuchen, eine PIN einzurichten.
536870953	Die angegebene PIN ist zu lang oder zu kurz. Dieser Antwort-Code wird nur für Funktionen angewandt, die versuchen, eine PIN einzurichten.
536870954	Die angegebene PIN ist geblockt und kann nicht genutzt werden. Dies tritt auf, weil eine gewisse Anzahl an fehlgeschlagenen Versuchen zur Authentisierung aufgetreten ist und der Token weitere Versuche zur Authentisierung ablehnt.
536870955	Die angegebene Slot ID ist ungültig.
536870956	Der Token war zu dem Zeitpunkt, als die Funktion angefragt wurde nicht in seinem Slot.
536870957	Das CBI Archiv und/oder der Slot konnte keinen Token im Slot erkennen.
536870958	Die angefragte Aktion kann nicht durchgeführt werden, da der Token schreibgeschützt ist.
536870959	Der angegebene Benutzer kann nicht angemeldet werden, da dieser Benutzername bereits zur Sitzung angemeldet ist.
536870960	Der angegebene Benutzer kann nicht angemeldet werden, da ein anderer Benutzer bereits zur Sitzung angemeldet ist.
536870961	Die gewünschte Aktion kann nicht ausgeführt werden, da der geeignete Benutzer (oder ein geeigneter Benutzer) nicht angemeldet ist. Zum Beispiel kann die Abmeldung von der Sitzung nicht vor der Anmeldung liegen.
536870962	Die normale Benutzer PIN ist nicht mit CBIInitPin initialisiert.
536870963	Es wurde versucht, gleichzeitig mehrere verschiedene Benutzer auf dem Token anzumelden, was der Token und/oder das Archiv zugelassen haben.

536870964	Ein ungültiger Wert wurde als CBIUser angegeben. Gültige Typen sind in ASCI11 User Types definiert.
536870965	Ein Objekt mit der angegebenen Kennzeichnung konnte auf dem Token nicht gefunden werden.
536870966	Eine Zeitüberschreitung ist aufgetreten.
536870967	Diese Version der IE ist nicht unterstützt.
536870968	Authentisierung fehlgeschlagen.
536870969	Das Root-Zertifikat ist gesichert.
536870970	Keine CRL gefunden.
536870971	Keine aktive Internetverbindung vorhanden.
536870972	Es befindet sich ein Fehler im Zeitwert eines Zertifikates.
536870973	Das Zertifikat konnte nicht verifiziert werden.
536870974	Der Aufhebungsstatus dieses Zertifikates ist unbekannt.
536870975	Das Modul wird beendet. Keine weiteren Anfragen gestattet.
536870976	Es ist ein Fehler während einer Netzwerkfunktion aufgetreten.
536870977	Ein ungültiger Aufruf einer Funktion ist empfangen worden.
536870978	Ein Objekt konnte nicht gefunden werden.
536870979	Eine Terminal Server Sitzung wurde unterbrochen.
536870980	Ungültige Handlung.
536870981	Das Objekt ist in Benutzung.
536870982	Der Zufallszahlengenerator wurde nicht initialisiert. (CBIRNDInit ( ) wurde nicht angefragt.)
536870983	Unbekannter Befehl (siehe CBIControl ( )).
536870984	UNICODE wird nicht unterstützt.
536870985	Der Zufallszahlengenerator benötigt einen größeren Startwert (seed).
536870986	Das Objekt existiert bereits.
536870987	Falsche Algorithmus Kombination. (Siehe CBIRecrypt ( )).
536870988	Das Cryptoki-Modul (PKCS#11) ist nicht initialisiert.
536870989	Das Cryptoki-Modul (PKCS#11) ist bereits initialisiert.
536870990	Das Cryptoki-Modul (PKCS#11) konnte nicht geladen werden.
536870991	Zertifikat nicht gefunden.
536870992	Nicht vertrauenswürdig.

536870993	Ungültiger Schlüssel.
536870994	Der Schlüssel ist nicht exportierbar.
536870995	Der angegebene Algorithmus wird momentan nicht unterstützt.
536870996	Der angegebene Entschlüsselungsmodus wird nicht unterstützt.
536870997	Ein Fehler in der GSENC Sammlung ist aufgetreten.
536870998	Format der Datenabfrage ist nicht bekannt.
536870999	Das Zertifikat hat keinen privaten Schlüssel.
536871000	Ungültige Konfiguration
536871001	Eine Operation ist aktiv.
536871002	Ein Zertifikat in der Kette ist zeitlich nicht verschachtelt.
536871003	Die CRL konnte nicht ersetzt werden.
536871004	Die BENUTZER-PIN wurde bereits initialisiert.
805306369	Sie haben keine ausreichenden Rechte, um diese Aktion auszuführen. Zugriff verweigert
805306370	Ungültiger Handle
805306371	Ungültiger Parameter in Benutzung
805306372	Das Objekt existiert bereits.
805306373	Das Objekt konnte nicht gefunden werden.
805306374	Datenbank-Ausnahme aufgetreten.
805306375	Die Aktion wurde vom Benutzer abgebrochen.
805306376	Das Token ist keinem bestimmten Benutzer zugewiesen.
805306377	Das Token ist mehr als einem Benutzer zugewiesen.
805306378	Das Token konnte nicht in der Datenbank gefunden werden.
805306379	Das Token wurde erfolgreich gelöscht und aus der Datenbank entfernt.
805306380	Das Token konnte in der Datenbank nicht eindeutig identifiziert werden.
805306381	Die Richtlinie ist einer Richtlinien-Gruppe zugewiesen. Um die Richtlinie zu löschen, muss diese Zuweisung aufgehoben werden.
805306382	Die Richtlinie ist einer OU zugewiesen. Bitte entfernen Sie zuerst die Zuweisung.
805306383	Das Zertifikat dieses Beauftragten ist ungültig.
805306384	Das Zertifikat dieses Beauftragten ist abgelaufen.
805306385	Der Beauftragte konnte nicht in der Datenbank gefunden werden.

805306386	Der gewählte Beauftragte ist nicht eindeutig.
805306387	Der Beauftragte ist gesperrt und kann nicht authentisiert werden.
805306388	Der Beauftragte ist nicht mehr oder noch nicht gültig.
805306389	Der Beauftragte konnte nicht authentisiert werden - Anfrage außerhalb der gestatteten Arbeitszeiten.
805306390	Ein Beauftragter kann sich nicht selbst löschen.
805306391	Der Haupt-Sicherheitsbeauftragte kann nicht gelöscht werden, da ein zweiter Haupt-Sicherheitsbeauftragte zur zusätzlichen Authentisierung erforderlich ist.
805306392	Der Sicherheitsbeauftragte kann nicht gelöscht werden, da ein zweiter Sicherheitsbeauftragte zur zusätzlichen Authentisierung erforderlich ist.
805306393	Der Prüfungsbeauftragte kann nicht gelöscht werden, da ein weiterer Prüfungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306394	Der Recovery-Beauftragte kann nicht gelöscht werden, da ein Recovery-Beauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306395	Der Beratungsbeauftragte kann nicht gelöscht werden, da ein Beratungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306396	Die Funktion des Haupt- Sicherheitsbeauftragten kann nicht entfernt werden, da ein zweiter Haupt-Sicherheitsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306397	Die Funktion des Sicherheitsbeauftragten kann nicht entfernt werden, da ein Sicherheitsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306398	Die Funktion des Prüfungsbeauftragten kann nicht entfernt werden, da ein Prüfungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306399	Die Funktion des Wiederherstellungsbeauftragten kann nicht entfernt werden, da ein Recovery-Beauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306400	Die Funktion des Beratungsbeauftragten kann nicht entfernt werden, da ein Beratungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306401	Ein zusätzlicher Beauftragter mit der gewünschten Funktion ist zur zusätzlichen Authentisierung nicht verfügbar.
805306402	Ereignisanzeige
805306403	Integrität des zentralen Ereignisprotokolls erfolgreich verifiziert.
805306404	Integrität verletzt! Ein oder mehrere Ereignisse wurden vom Beginn der Kette entfernt.

805306405	Integrität verletzt! Ein oder mehrere Ereignisse sind in der Kette entfernt worden. Die Mitteilungen bei denen der Bruch der Kette entdeckt worden ist, ist hervorgehoben.
805306406	Integrität verletzt! Ein oder mehrere Ereignisse wurden vom Ende der Kette entfernt.
805306407	Exportieren der Ereignisse in Datei fehlgeschlagen. Grund:
805306408	Die momentane Ansicht enthält ungesicherte Daten. Möchten Sie die Änderungen speichern, bevor Sie die Ansicht verlassen?
805306409	Die Datei konnte nicht geladen werden, oder die Datei ist beschädigt. Grund:
805306410	Die Integrität des Protokolls ist verletzt worden! Ein oder mehrere Ereignisse sind entfernt worden.
805306411	Sollen die Ereignisse in einer Datei gesichert werden, bevor sie gelöscht werden?
805306412	Anzeige der Aufträge
805306413	CRL mehrfach in der Datenbank gefunden. CRL konnte nicht gelöscht werden.
805306414	CRL nicht in der Datenbank gefunden.
805306415	Der Benutzer, dem das Zertifikat zugewiesen werden sollte, konnte nicht in der Datenbank gefunden werden.
805306416	Ein P7 Blob ist für eine Zertifikats-Zuweisung zwingend erforderlich.
805306417	Der Benutzer, dem das Zertifikat zugewiesen werden sollte, ist nicht eindeutig benannt.
805306418	Die Zertifikats-Zuweisung kann nicht gefunden werden.
805306419	Die Zuweisung des Zertifikats ist nicht eindeutig. Es ist nicht klar, welche Zuweisung entfernt werden soll.
805306420	Der Benutzer für den das Zertifikat erstellt werden soll, konnte nicht in der Datenbank gefunden werden.
805306421	Der Benutzer für den das Zertifikat erstellt werden soll, kann nicht eindeutig benannt werden.
805306422	Das Zertifikat wurde bereits einem anderen Benutzer zugeordnet. Ein Zertifikat kann nur einem Benutzer zugeordnet werden.
805306423	Der Computer, dem das Zertifikat zugewiesen werden soll, konnte nicht in der Datenbank gefunden werden.
805306424	Der Computer, dem das Zertifikat zugewiesen werden soll, konnte nicht eindeutig identifiziert werden.

805306425	Importierte Zertifikate können nicht durch SGN erneuert werden.
805306426	Inkonsistente Zertifikatsdaten während der Erneuerung
805306427	Die Erneuerung des Zertifikats wurde nicht von einem Sicherheitsbeauftragten genehmigt.
805306428	Fehler beim Löschen des Token
805306429	Das Zertifikat kann nicht vom Token gelöscht werden, denn es wurde für die Authentisierung des aktuellen Benutzers verwendet.
805306430	Ein Systemzugang mit diesem Namen existiert bereits. Bitte wählen Sie einen anderen Namen.
805306431	Dem Sicherheitsbeauftragen sind keine Rollen zugewiesen. Anmeldung nicht möglich.
805306432	Die Lizenz wurde verletzt.
805306433	Es wurde keine Lizenz gefunden.
2415919104	Es wurde keine Richtlinie gefunden.
2415919105	Keine Konfigurationsdatei verfügbar!
2415919106	Keine Verbindung zum Server.
2415919107	Keine weiteren Datenpakete vorhanden.
2415919108	Ungültige Priorität beim Senden zum Server!
2415919109	Es stehen noch Daten zur Verarbeitung an.
2415919110	Die Autoregistrierung ist noch nicht beendet.
2415919111	Datenbank Anmeldung fehlgeschlagen.
2415919112	Falsche Session ID!
2415919113	Datenpaket ignoriert!
3674210305	Domäne nicht gefunden.
3674210306	Maschine nicht gefunden.
3674210307	Benutzer nicht gefunden.
3758096385	Das Kennwort enthält nicht genügend Buchstaben
3758096386	Das Kennwort enthält nicht genügend Zahlen
3758096387	Das Kennwort enthält nicht genügend Sonderzeichen
3758096388	Das Kennwort entspricht dem Benutzernamen
3758096389	Das Kennwort enthält aufeinanderfolgende Zeichen
3758096390	Das Kennwort ähnelt dem Benutzernamen zu stark
3758096391	Das Kennwort wurde in der Liste der verbotenen Kennwörter gefunden

3758096392	Das Kennwort ähnelt dem alten Kennwort zu stark
3758096393	Das Kennwort enthält eine Tastaturreihe mit mehr als zwei Zeichen
3758096394	Das Kennwort enthält eine Tastaturspalte mit mehr als zwei Zeichen
3758096395	Das Kennwort hat seinen Gültigkeitszeitraum noch nicht erreicht
3758096396	Das Kennwort hat seine Gültigkeitsdauer überschritten
3758096397	Das Kennwort hat seine minimale Gültigkeitsdauer noch nicht erreicht
3758096398	Das Kennwort hat die maximale Gültigkeitsdauer überschritten
3758096399	Information über einen bevorstehenden Wechsel des Kennwortes muß angezeigt werden
3758096400	Änderung bei Erstanmeldung erforderlich
3758096401	Das Kennwort wurde in der History gefunden
3758096402	Fehler beim Verifizieren gegen die spezifizierte Blacklist.
4026531840	Keine "platform" vorhanden.
4026531841	Kein Dokument.
4026531842	XML Parse Fehler.
4026531843	Fehler im Document Object Model (XML).
4026531844	Kein <DATAROOT>-Abschnitt gefunden (XML).
4026531845	XML-Tag nicht gefunden.
4026531846	"nostream" Fehler.
4026531847	"printtree" Fehler.

31 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter http://community.sophos.com auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter http://www.sophos.de/support/.
- Laden Sie Dokumentation zu den Produkten unter http://www.sophos.de/support/docs/ herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

32 Copyright

Copyright © 1996 - 2010 Sophos Group und Utimaco Safeware AG. Alle Rechte vorbehalten.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos ist ein eingetragenes Warenzeichen von Sophos Plc und der Sophos Group. SafeGuard ist ein eingetragenes Warenzeichen von Utimaco Safeware AG - a member of the Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Alle SafeGuard Produkte unterliegen dem Urheberrecht der Utimaco Safeware AG - a member of the Sophos Group, oder, sofern anwendbar, ihrer Lizenzinhaber. Alle weiteren Sophos Produkte unterliegen dem Urheberrecht der Sophos Plc oder, sofern anwendbar, ihrer Lizenzinhaber.

Copyright-Informationen von Drittanbietern finden Sie in der Datei *Disclaimer and Copyright for 3rd Party Software.rtf* in Ihrem Produktverzeichnis.